



CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRE

Achat de services de cloud public PAAS
dans un environnement de confiance

Mars 2024



Cigref

Cahier des clauses techniques particulières

*Achat de services de cloud public PAAS dans
un environnement de confiance*

Juin 2024



Droit de propriété intellectuelle

Toutes les publications du Cigref sont mises gratuitement à la disposition du plus grand nombre mais restent protégées par les lois en vigueur sur la propriété intellectuelle

OBJECTIF

Un certain nombre de membres du Cigref envisagent de lancer un appel d'offres pour des solutions de cloud de confiance. C'est pourquoi nous avons décidé de travailler collectivement à la rédaction de la partie technique d'un tel appel d'offres, en prenant en compte le référentiel cloud de confiance du Cigref. En effet, les membres du Cigref ont exprimé leurs besoins génériques de confiance en tant qu'utilisateurs de services cloud dans le référentiel cloud de confiance dont la version³, version amendée par les utilisateurs et fournisseurs européens, est disponible [ici](#)¹. Les exigences ont été tirées de diverses références, dont SecNumcloud, Gaia-X et SWIPO, entre autres. Le présent document appelé Cahier des Clauses Techniques Particulières (CCTP), disponible également en anglais sous le nom *Technical Specifications Booklet* (TSB) est le résultat de la *Task Force*, sous-groupe du groupe de travail cloud de confiance du Cigref, composé d'entreprises et d'administrations publiques.

Le présent CCTP doit être intégré dans la demande de proposition (RFP) pour des services et solutions cloud de confiance. Le CCTP décrit les exigences et les attentes du client des services cloud (CSC pour cloud *Services Consumer*) pour l'acquisition d'un ensemble de services d'informatique en nuage de confiance (IaaS, PaaS, CaaS, FaaS et SaaS tels que définis ci-dessous). Le CCTP partage les besoins et les défis auxquels sont confrontées les entreprises et les administrations publiques en termes de sécurité, de contrôle de la dépendance vis-à-vis des fournisseurs, d'immunité vis-à-vis des lois non européennes, de contrôle de l'empreinte environnementale des services cloud et de confiance chez les fournisseurs cloud. Ces exigences intègrent les critères cloud "safe" et cloud "trusted" du référentiel cloud de confiance du Cigref.

Avant d'envoyer le CCTP au fournisseur de services cloud (CSP pour cloud *Service Provider*), **certaines parties surlignées en jaune** doivent être modifiées/complétées par le CSC afin de les adapter à ses besoins, son contexte et ses activités spécifiques. Il est important de noter que ce document est une référence et qu'il peut, bien sûr, être adapté au-delà des recommandations en supprimant ou en ajoutant de nouvelles sections et exigences.

Deux fichiers Excel complètent le CCTP.

1. Le fichier intitulé " Cigref_Conversion matrix Ref_ Trusted cloud RFP_2024 " garde la trace de l'origine des exigences dans le CCTP. Il permet de comprendre facilement d'où provient une exigence et de la retrouver sous sa forme originale dans le document de référence du cloud de confiance.
2. Le fichier intitulé " Cigref_TSB Answers grid_Trusted cloud RFP_2024 " est là pour aider le CSP dans ses réponses et le CSC dans son évaluation des réponses des fournisseurs. Afin de simplifier l'évaluation des CCTP, nous avons divisé les questions/exigences en deux types : les questions fermées « OUI-NON » et les questions ouvertes. Les questions ouvertes regroupent les questions qui nécessitent une réponse détaillée.

¹ <https://www.cigref.fr/cigref-publishes-its-third-version-of-the-trusted-cloud-reference-document>

TABLE DES MATIÈRES

1 INTRODUCTION ET CONTEXTE	5
1.1 Préambule	5
1.1.1 Objectif du document	5
1.1.2 Grille de lecture	5
1.1.3 Glossaire et acronymes.....	5
1.2 Cadre général	8
1.2.1 Contexte.....	8
1.2.2 Enjeux et objectifs.....	8
1.2.3 Description de la consultation	8
1.2.4 Exigences de localisation des données	9
1.2.5 Exigences de localisation de niveau de confiance	11
1.2.6 Synthèse des prestations attendues.....	11
1.2.7 Définition des services	11
1.2.8 Définition des utilisateurs.....	11
1.2.9 Planning	12
1.2.10 Synthèse des exigences de cloud de confiance.....	12
2 MODALITÉS DE LA PRESTATION	13
2.1. Expression de besoin du Service attendu	13
2.1.1. Fourniture de services de cloud <i>computing</i>	13
2.1.1 Modèles de déploiement	13
2.1.2 Modèles de Service	15
2.1.3 Facturation du service	15
2.1.4 Pilotage du service	17
2.1.5 Exigences techniques.....	17
2.1.5.1 Postes utilisateurs	17
2.1.5.2 IT Network	18
2.1.5.3 Interopérabilité avec le reste du SI et portabilité	19
2.2 Prestations attendues	20
2.2.1 Mise à disposition des services.....	20
2.2.2 Réversibilité et portabilité	20
2.2.3 Market place	33
2.2.4 Construction du socle d'infrastructure	33
2.3 Pilotage des services concernant l'operational readiness	35
2.3.1 Gestion de la disponibilité des services	35
2.3.2 Gestion de la continuité du service	36

2.3.3	Gestion de la performance du service	37
2.3.4	Évolution du service	37
2.3.5	Support	38
2.3.6	Gestion des incidents.....	40
2.3.7	Gestion des anomalies.....	45
2.3.8	Gestion des crises	45
2.3.9	Gestion des risques	46
2.3.10	Gestion des actifs	48
2.3.11	Sécurité des locaux et du personnel	49
2.3.12	Gestion des vulnérabilités	56
2.3.13	Opérabilité.....	56
2.4	Gouvernance et Gestion opérationnelle.....	60
2.4.1	gouvernance	60
2.4.2	Gestion de la qualité	60
2.4.3	Reporting et indicateurs	61
2.4.4	Comitologie.....	62
3	SÉCURITÉ	65
3.1	Exigences de sécurité	65
3.1.1	Politique de sécurité du système d'information (PSSI)	65
3.1.2	Plan d'assurance de sécurité (PAS).....	65
3.1.3	Contact de sécurité du système d'information (CSSI)	67
3.1.4	Mesures de contrôle et d'audit	68
3.1.5	Sécurité des informations.....	70
3.1.6	Chiffrement des données et certificats	73
3.1.7	Traçabilité	75
3.1.8	Partitionnement.....	77
3.1.9	Sécurité des communications.....	79
3.1.10	Patch de sécurité	80
3.1.11	Accès et identités	80
3.1.12	Acquisition, développement et maintenance des systèmes d'information.....	85
3.1.12.1	Analyse de code.....	85
3.1.12.2	API.....	86
3.1.13	Sous-traitance.....	86
3.1.14	Conformité	89
3.1.15	Services de sécurité.....	93
3.2	Exigences de sécurité de confiance	100

4 CATALOGUE DE SERVICES D'INFRASTRUCTURE ET DE FONDATIONS	104
4.1 services d' Infrastructure	104
4.1.1 Puissance de calcul	104
4.1.2 Gestion des configurations	105
4.1.3 Stockage et backup	106
4.1.4 Gestion des templates et ressources.....	107
4.2 Administration réseaux.....	107
5 CATALOGUE DE SERVICES MÉTIERS	109
5.1 Valorisation des données.....	109
5.1.1 Bases de données	109
5.1.2 Collecte et traitements des données.....	109
5.1.3 Analyse et restitution des données	110
5.1.4 Intelligence artificielle.....	111
5.2 Services de migration.....	113
5.3 Gestion applicative.....	114
5.3.1 DevSecOps	114
5.3.2 Services de contenu	118
5.3.3 Services applicatifs.....	119
5.4 Internet des objets.....	122
5.5 Services mobiles.....	123
5.6 Services entreprise.....	125
5.7 Services Finops.....	126
6 FOCUS ENVIRONNEMENTAL	127
6.1 Exigences énergétiques.....	127
6.2 émissions et empreinte carbone	128
6.3 Exigences de ressources hydrique et récupération de la chaleur	129
6.4 Exigences sur le cycle de vie des composants électroniques	130

1 INTRODUCTION ET CONTEXTE

1.1 PRÉAMBULE

1.1.1 OBJECTIF DU DOCUMENT

Le présent cahier des clauses techniques particulières (CCTP) décrit les exigences du client de services cloud (CSC pour cloud *Services Consumer*). Il détaille leurs attentes pour l'acquisition d'un ensemble de services cloud de confiance (IaaS, PaaS, CaaS, SaaS tels que définis ci-dessous), désigné dans le reste du document comme le SERVICE.

La future entreprise attributaire du contrat correspondant à ce CCTP est désignée dans le présent document comme le fournisseur de services cloud (CSP pour cloud *Services Provider*).

1.1.2 GRILLE DE LECTURE

Le présent document détaille, sous forme d'exigences, les attentes du CSC à l'égard du CSP. Chaque exigence est présentée selon le formalisme suivant :

Identifiant unique de l'exigence	Description courte de l'exigence	
Description complète de l'exigence		
Livrable(s)	Contrôle des résultats	Niveau à atteindre
<ul style="list-style-type: none"> Livrables associés à l'exigence 	<ul style="list-style-type: none"> Indicateur ou procédure de contrôle 	<ul style="list-style-type: none"> Niveau de service à atteindre Écart de performance associé

Les prestations liées à certaines exigences décrites dans le présent CCTP sont parfois précisées dans les Conditions Particulières d'Achat (CPA) avec les pénalités associées.

1.1.3 GLOSSAIRE ET ACRONYMES

Les acronymes suivants sont utilisés dans le CCTP :

Acronyme	Définition	Acronyme anglais
PCA	Plan de continuité d'activité	Business Continuity Plan (BCP)
CSA	Contrat de services	Contract Service Agreement (CSA)
CSC	Entreprise consommatrice de services cloud	cloud Service Customer

Acronyme	Définition	Acronyme anglais
CSP	Fournisseur de services cloud	Cloud Service Provider
FQDN	Nom de domaine complet	Fully Qualified DNS Name (FQDN)
IHM	Interface Homme Machine	Human-machine interface (HMI)
PSSI	Politique Sécurité du SI	Information System Safety Policy (ISSP)
RSSI	Responsable Sécurité du Système d'Information	Information System Safety Responsible (ISSR)
ITIL	ITIL	Information Technology Infrastructure Library
MFA	Authentification multi-facteurs	Multi-Factor Authentication
NDA	Accord de confidentialité	Non-Disclosure Agreement
OS	Système d'exploitation	Operating System
PAQ	Plan d'assurance qualité	Quality Assurance Plan (QAP)
PAQS	Plan Assurance Qualité et Sécurité	Quality and Safety Assurance Plan (QSAP)
PAS	Plan Assurance Qualité et Sécurité	Safety Assurance Plan (SAP)
SLA	Engagement de service	Service Level Agreement
SLO	Objectifs de niveau de services	Service Level Objective
SQO	Objectif qualitatif du service	Service Qualitative Objective (SQO)
CPA	Conditions Particulières d'Achat	Terms and Conditions of Purchase (TCP)
CCTP	Cahier des Clauses Techniques Particulières	Technical Specifications Booklet (TSB)
VM	Machine Virtuelle	Virtual Machine (VM)
VPC	Nuage privé virtuel	Virtual Private Cloud (VPC)

Les termes suivants seront utilisés dans le CCTP.

Terme	Définition	English Term
Administration	Ensemble des gestes techniques permettant la gestion en termes de maintenance, d'amélioration et de supervision afin de faire évoluer une infrastructure, un OS ou un logiciel.	Administration

Terme	Définition	English Term
API	<i>Application Programming Interface</i> Interface permettant (dans le contexte du présent CCTP) d'accéder de manière programmatique aux services cloud du CSP	API
CaaS	<i>Container as a Service</i> Modèle de services de cloud <i>computing</i> où le CSP fournit l'hébergement et éventuellement l'orchestration de containers Docker	CaaS
Cloud broker	Entité ou entreprise jouant le rôle d'intermédiaire entre les consommateurs finaux de services de cloud et les fournisseurs de ces services	Cloud Broker
CMP	<i>Cloud Management Platform</i> Solution logicielle permettant de gérer de manière unifiée et centralisée une ou plusieurs plateformes de <i>cloud computing</i>	CMP
Exploitation	Ensemble des gestes techniques réalisés pour assurer la continuité de service d'une infrastructure, d'un OS ou d'un logiciel, sans en faire évoluer la configuration, sauf si nécessaire à la résolution d'un incident	Exploitation
Export	Exportation des données du cloud vers le CSC	Export
FaaS	<i>Function as a service</i> Catégorie de services de cloud où le CSP fournit une plate-forme permettant au CSC de développer, d'exécuter et de gérer les fonctionnalités.	FaaS
Cloud Hybride	Utilisation simultanée et intégrée de multiples offres de cloud <i>computing</i> : privé ou public, interne ou externe	Hybrid cloud
IaaS	<i>Infrastructure as a Service</i> Modèle de services de cloud <i>computing</i> où le CSP fournit des infrastructures (machines virtuelles, éléments d'infrastructure réseaux, stockage, etc.) à ses utilisateurs ; il exploite et administre l'infrastructure physique et virtuelle sous-jacente.	IaaS
Import	Importation des données du CSC vers le cloud	Import
PaaS	<i>Platform as a Service</i>	PaaS

Terme	Définition	English Term
	Modèle de services de cloud <i>computing</i> où le CSP fournit des plateformes pouvant accueillir les applications développées par ses utilisateurs ; il exploite et administre l'infrastructure (OS compris) ainsi que les logiciels sous-jacents.	
Portabilité	Le droit pour tout consommateur de récupérer l'ensemble de ses données et de les transférer à un autre opérateur tout en continuant à utiliser le service	Portability
Réversibilité	Le droit de tout consommateur de récupérer toutes ses données et de les transférer à un autre opérateur en cas de résiliation du contrat	Reversibility

1.2 CADRE GÉNÉRAL

1.2.1 CONTEXTE

Cette partie doit être remplie par le CSC, en décrivant son contexte particulier et les exigences spécifiques à adresser au CSP.

1.2.2 ENJEUX ET OBJECTIFS

Cette partie doit être remplie par le CSC, en décrivant ses problèmes et ses attentes spécifiques à l'égard du CSP. Voici un exemple :

- Performance :** Réduction des coûts grâce à la facturation à l'usage, typique d'un cloud public ;
Possibilité de construire des applications chez un fournisseur externe ;
- Agilité :** Élasticité apportée par des ressources supplémentaires rapidement disponibles en cloud public ;
Rapidité d'évolution et d'enrichissement des catalogues de services des fournisseurs cloud public ;
- Innovation :** Possibilité d'expérimentation sur un environnement ouvert et externe au CSC ;
- Confiance :** Ce document contient des exigences impliquant un environnement cloud de confiance, y compris des clauses sur l'immunité, la transparence, l'intégrité et la confidentialité ;

1.2.3 DESCRIPTION DE LA CONSULTATION

Cette partie doit être remplie par le CSC, en décrivant ses problèmes et ses attentes spécifiques à l'égard du CSP. Voici un exemple :

La consultation menée par le CSC est construite en fonction des cas d'usages envisagés par le CSC, qui sont associés à différents modèles de Services cloud.

En complément d'un modèle de services IaaS, les modèles de services PaaS, CaaS, FaaS et SaaS sont également requis.

Les cas d'usages identifiés par le CSC pour la consultation sont :

- L'approvisionnement d'environnements critiques et non critiques, y compris les environnements de production utilisés 24h/24, 7j/7 ;
- Les ressources, ainsi approvisionnées, hébergent notamment des applications événementielles (durées de vie de quelques semaines à quelques mois) ;
- Les applications développées, testées et mises en production sur l'infrastructure du CSP tirent parti de la richesse de son catalogue de services ;
- LE CSC souhaite également pouvoir expérimenter des services proposés sur les plateformes du CSP.

1.2.4 EXIGENCES DE LOCALISATION DES DONNÉES

LOC-1	Le CSP doit respecter les exigences en matière de localisation des données	
<p>Afin de se conformer à la législation européenne en matière de protection des données à caractère personnel, le CSC souhaite identifier et limiter les localisations possibles des données qu'il transfère à l'infrastructure du CSP. Dans ce contexte, la zone géographique de référence est constituée par :</p> <ul style="list-style-type: none"> • Les pays membres de l'Union européenne (UE) ou de l'Espace économique européen (EEE) : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Slovaquie, Slovénie et Suède. <p>Le CSP doit communiquer :</p> <ul style="list-style-type: none"> • la localisation de ses actifs (précision requise : au niveau de la ville). • la localisation de ses centres de données • ses actionnaires et leur localisation • la localisation de son siège social. <p>Le CSP doit également informer le CSC si l'un des centres de données qui stocke ou traite les données et les services du CSP sera déplacé ou fermé.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Localisations et liste des actionnaires 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Les centres de données du CSP doivent être situés dans l'Union européenne. • Le siège social, l'administration centrale et l'établissement

		principal du CSP doivent être établis dans un État membre de l'Union européenne.
--	--	--

LOC-2 	Le CSP fournit au CSC la preuve de la mise en œuvre de garanties appropriées régissant les transferts de données en dehors de l'UE.	
<p>Le CSP ne doit pas transférer de données à caractère personnel à un pays tiers ou à une organisation internationale sans l'accord écrit préalable du CSC.</p> <p>Si les données sont susceptibles d'être transférées en dehors de l'Union européenne ou de l'Espace économique européen, le CSP apporte la preuve que des garanties appropriées régissent ces transferts. Ces garanties peuvent être des règles contraignantes du CSC ou des clauses contractuelles types de la Commission européenne.</p> <p>Le règlement général sur la protection des données (RGPD) stipule que le transfert de données vers un pays tiers ne peut avoir lieu que si le pays tiers garantit un niveau adéquat de protection des données. En l'absence de décision d'adéquation, le transfert ne peut avoir lieu que si l'exportateur de données, établi dans l'UE, fournit des garanties appropriées, qui peuvent inclure des clauses types de protection des données adoptées par la Commission, et si les personnes concernées disposent de droits exécutoires et de voies de recours effectives.</p> <p>Avant tout transfert, l'exportateur de données (CSC) et le destinataire (CSP) doivent vérifier que le pays tiers respecte le niveau de protection requis par la législation européenne. Les CSC dont les données personnelles sont transférées vers un pays tiers sur la base de clauses types de protection des données doivent bénéficier d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'UE par ce règlement, lu à la lumière de la Charte de l'UE.</p> <p>Le CSP doit mettre en œuvre des mécanismes efficaces (clauses standards de protection) pour garantir que le niveau de protection requis par la législation de l'UE est respecté dans la pratique. Les transferts de données à caractère personnel fondés sur ces clauses doivent être suspendus ou interdits en cas de violation de ces clauses ou s'il est impossible de les respecter.</p> <p>Enfin, le CSP doit informer immédiatement le CSC si le lieu de traitement des données change par rapport à celui spécifié dans l'accord pour des raisons relevant du domaine de responsabilité du CSP pendant la durée de validité de l'accord de service.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> L'engagement du CSP 	<ul style="list-style-type: none"> Vérification de l'engagement du CSP 	<ul style="list-style-type: none"> Vérification de l'engagement du CSP

1.2.5 EXIGENCES DE LOCALISATION DE NIVEAU DE CONFIANCE

LOC-3	Le CSP doit indiquer la localisation de tout sous-traitant susceptible d'accéder aux données du CSC.	
Le CSP doit indiquer la localisation de tout sous-traitant susceptible d'accéder aux données du CSC.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Localisation des sous-traitants 	<ul style="list-style-type: none"> Réception des documents par le CSP 	<ul style="list-style-type: none"> <u>Niveau minimal attendu</u> : Le CSP communique la ville des sous-traitants. <u>Niveau de confiance requis</u> : Le CSP n'a pas de sous-traitant en dehors de l'Union européenne qui puisse accéder aux données du CSC.

1.2.6 SYNTHÈSE DES PRESTATIONS ATTENDUES

Le CSP réalise les prestations suivantes :

- Hébergement et exploitation des services ;
- Accès aux services ;
- Evolution des services ;
- Support et assistance sur les services ;
- Mise à disposition d'un service de pilotage et de gestion des coûts ;
- Mise en place du socle d'infrastructure pour accueillir les applications en toute sécurité ;
- Mise en place de mesures de réversibilité et portabilité ;
- Mise en place de mesures renforcées de sécurité de confiance ;
- Mise en place de mesures d'immunité.

Le CSP réalise le pilotage opérationnel de ces prestations et participe à la Gouvernance des services.

1.2.7 DÉFINITION DES SERVICES

Dans le présent document, l'expression les « services » désigne l'ensemble du catalogue de services informatiques d'un seul CSP (cloud Service Provider) fourni par le CSP à ses clients : il s'agit de tous les services des modèles IaaS, PaaS, SaaS, FaaS et SaaS. En fonction du contexte des exigences, des services spécifiques peuvent être spécifiés.

1.2.8 DÉFINITION DES UTILISATEURS

Cette partie peut être modifiée pour se conformer à la définition spécifique des utilisateurs du CSC.

Les utilisateurs du CSC susceptibles d'accéder aux SERVICES sont de deux types :

1. Les administrateurs des services cloud *computing*

Cahier des clauses techniques particulières

Achat de services de cloud public PAAS dans un environnement de confiance



Ils intégreront les SERVICES aux offres de services cloud du CSC

Ils doivent disposer des rôles aux droits d'administration les plus avancés, être formés à l'utilisation des services, être informés des évolutions et des incidents qui affectent les services.

Pour le CSC, ils serviront d'intermédiaires entre le CSP et les utilisateurs finaux des SERVICES.

Le CSP mettra à disposition les outils et les canaux de communication avec le CSC pour administrer les services, et disposer d'informations en cas de changement ou d'incident.

2. Les utilisateurs finaux des services cloud *computing*

Ce sont les utilisateurs du CSC consommateurs des services du CSP (par exemple développeurs).

En particulier, ils pourront consommer ces services à travers soit d'une CMP du CSC, soit via le portail ou API du CSP.

Ils doivent disposer de rôles limités (capacité d'approvisionnement limitée) paramétrés par les administrateurs, et ne seront pas en contact direct avec le CSP.

Outre les utilisateurs du CSC, les ressources hébergées chez le CSP exposées sur Internet sont également susceptibles d'être accédées par des **utilisateurs publics**, externes au CSC.

1.2.9 PLANNING

Le CSP s'engage sur le respect des délais, du planning et des jalons convenus avec le CSC.

Le CSP s'engage à respecter la date d'ouverture des SERVICES **dès la signature du marché**

Les principales activités engageant le CSP sont :

- Mise à disposition d'un socle d'infrastructure permettant aux utilisateurs des SERVICES de déployer des applications ;
- Mise en place des processus de communications avec les administrateurs du CSC ;
- Mise en place des processus de relation commerciale avec le CSC.

1.2.10 SYNTHÈSE DES EXIGENCES DE CLOUD DE CONFIANCE

Ce CCTP comprend un certain nombre d'exigences supplémentaires axées sur les "services en nuage de confiance". Certaines d'entre elles sont "optionnelles" et leur respect se traduira par des points supplémentaires. Cependant, certaines d'entre elles ont été jugées essentielles et le fait de ne pas pouvoir s'y conformer peut entraîner une détérioration significative de l'évaluation.

Une mention spéciale apparaîtra lorsque la conformité à l'une de ces exigences de cloud de confiance sera jugée "essentielle".


2 MODALITÉS DE LA PRESTATION

2.1. EXPRESSION DE BESOIN DU SERVICE ATTENDU

2.1.1. FOURNITURE DE SERVICES DE CLOUD *COMPUTING*

FCT-1	Le CSP fournit un catalogue de services cloud	
<p>Le CSP fournit des services cloud regroupés et accessibles par le biais d'un catalogue de services.</p> <p>Chaque élément de ce catalogue de services correspond à un ensemble d'actions techniques automatisées réalisables à la demande par les clients du CSP. Il doit faire l'objet d'une description précise par le CSP, comprenant un libellé, une description, un ensemble de prérequis, des SLA (<i>Service Level Agreements</i> ou engagement de service), et d'éventuelles limitations.</p> <p>Ce catalogue comprend tous les services relevant des modèles de services IaaS, PaaS, CaaS, FaaS, SaaS, ainsi que les services d'inventaire, de surveillance et de facturation qui leur sont associés. Exclusivement défini par le CSP et sous sa seule responsabilité, ce catalogue est publié sur une interface utilisateur accessible via un client léger (navigateur web, au minimum Microsoft Edge, Chrome, et Firefox), ainsi que via des API. Il est proposé à tous les clients des CSP de manière standardisée et identique.</p> <p>Le CSP doit être en mesure de fournir tout ou partie de son catalogue de services (désigné dans le présent CCTP par "les SERVICES") en fonction des besoins du CSC.</p>		
Livraison(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Catalogue des services cloud du CSP 	<ul style="list-style-type: none"> Accès aux éléments du catalogue de services du CSP par le CSC (ce catalogue est différent de la Marketplace, plus de détails au paragraphe 2.2.3). 	<ul style="list-style-type: none"> Le catalogue des services du CSP, disponible auprès du CSC 24h/24, 7j/7 pendant toute la durée du marché.

2.1.1 MODÈLE DE DÉPLOIEMENT

FCT-2 	Le CSP fournit des services en cloud public
<p>A l'exception des infrastructures mises en place ou utilisées par le CSC pour accéder aux services (notamment les infrastructures d'interconnexion des réseaux et les postes de travail des utilisateurs), les services reposent sur des infrastructures louées ou détenues par le CSP.</p>	

Ces infrastructures peuvent être mises en commun et partagées entre tous les clients du CSP, selon un degré de mutualisation que le CSP définit et communique au CSC.

Dans le cas de besoins spécifiques, le CSP doit pouvoir offrir des services dédiés au CSC. Le CSP fournira une liste de services du catalogue qui peuvent être utilisés de cette manière.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Recommandations en matière de configuration du réseau et configuration des postes de travail des utilisateurs nécessaires à l'utilisation des services. 	<ul style="list-style-type: none"> Documentation à recevoir par le CSC 	<ul style="list-style-type: none"> Réception à valider
<ul style="list-style-type: none"> Informations sur le degré de partage de l'infrastructure entre les clients, sur la base des services figurant dans le catalogue de services du CSP. 	<ul style="list-style-type: none"> Documentation à recevoir par le CSC 	<ul style="list-style-type: none"> Réception à valider

FCT-3	Le CSP permet au CSC de choisir l'emplacement des données	
<p>Le CSP offre au minimum le choix entre 2 régions (situées géographiquement au sein de l'Union Européenne ou de l'Espace Economique Européen (cf. liste complète au chapitre 1)). Une région est un emplacement physique dans le monde où sont regroupés des centres de données. Chaque région se compose de zones de disponibilité multiples, isolées et physiquement séparées au sein d'une zone géographique. Chaque zone de disponibilité est composée d'un ou de plusieurs centres de données équipés d'une alimentation, d'un système de refroidissement et d'un réseau indépendant. Le CSC doit pouvoir localiser ses données de manière exclusive dans ces 2 régions.</p> <p>Le CSP doit pouvoir garantir à tout moment la localisation des données du CSC quel que soit leur nature au repos et en transit.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Liste des localisations de datacenters (au minimum : le pays) hébergeant l'infrastructure cloud Public du CSP 	<ul style="list-style-type: none"> Documentation à réceptionner par le CSC 	<ul style="list-style-type: none"> Réception à valider

2.1.2 MODÈLES DE SERVICE

FCT-4	Le CSP fournit des services cloud de type IaaS, PaaS, CaaS, FaaS, SaaS	
<p>Le CSP fournit à travers son catalogue de services les infrastructures nécessaires au déploiement des logiciels et applications du CSC : ce sous-ensemble du catalogue de services constitue les services cloud de type IaaS.</p> <p>Le CSP fournit à travers son catalogue de services, l'infrastructure et les logiciels nécessaires au déploiement des applications du CSC : ce sous-ensemble du catalogue de services constitue les services cloud de type PaaS.</p> <p>Le CSP fournit à travers son catalogue de services, l'infrastructure et les logiciels nécessaires au déploiement de containers : ce sous-ensemble du catalogue de services constitue les services cloud de type CaaS.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP fournit à travers son catalogue de services, une plateforme permettant au CSC de développer, d'exécuter et de gérer les fonctionnalités : ce sous-ensemble du catalogue de services constitue les services cloud de type FaaS.</p> <p>Le CSP fournit à travers son catalogue de service, une plateforme permettant la contractualisation, le suivi et la gestion de solutions SaaS éditées par le CSP ou par des tiers dont le CSP c'est assuré qu'ils respectent les mêmes exigences que pour les sous-traitants détaillés dans le paragraphe 3.1.13.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Liste des services cloud de type IaaS, PaaS, CaaS, FaaS, SaaS 	<ul style="list-style-type: none"> Documentation à réceptionner par le CSC 	<ul style="list-style-type: none"> Réception à valider

2.1.3 FACTURATION DU SERVICE

FAC-1	Le CSP facture l'utilisation des services en fonction de l'usage réel du CSC	
<p>Pour l'ensemble des articles à son catalogue de services, le CSP propose au CSC une facture mensuelle relative à l'activité du mois précédent (« M-1 »), dans les cinq premiers jours ouvrés du mois M.</p> <p>Cette facturation doit être complètement détaillée, sans ambiguïté, et vérifiable en s'appuyant sur des éléments mesurables tels que :</p> <ul style="list-style-type: none"> - La volumétrie de ressources consommées (puissance de calcul, stockage, bande-passante réseau...); - La durée d'utilisation de chaque service consommé au catalogue ; - Le nombre d'utilisateurs ayant eu accès service ; 		

- Le détail de la consommation au niveau du projet ou du compte ;
- Ainsi que tout autre élément nécessaire pour justifier de la facturation.

Le CSP doit rappeler dans ses propositions de factures le détail de ces éléments mesurables ayant conduit aux montants facturés. Seuls les articles du catalogue de services du CSP ayant été requis par le CSC doivent être facturés. Le modèle initial du fichier de facturation fera l'objet d'une validation du CSC en phase de mise à disposition et le CSP devra de même notifier le CSC et obtenir la validation du CSC pour toute évolution ultérieure en cours de marché.

Le CSP communique des notes de crédit proportionnelles à la facturation du mois en cours, en compensation de l'indisponibilité du service ou de la non-conformité au cours du mois précédent.

Le CSP fournit et met à jour un outil de simulation en ligne permettant au CSC d'anticiper son coût d'utilisation du service.

Le CSP met à disposition des outils permettant au CSC de gérer et d'optimiser sa consommation financière et ses coûts de services cloud.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Proposition de facturation mensuelle 	<ul style="list-style-type: none"> • Proposition de facturation à réceptionner par le CSC 	<ul style="list-style-type: none"> • Proposition de facturation doit être conforme à l'activité du CSC du mois M-1, et reçue dans les 5 premiers jours du mois M
<ul style="list-style-type: none"> • Modèle de fichier de facturation 	<ul style="list-style-type: none"> • Modèle de fichier de facturation à réceptionner par le CSC 	<ul style="list-style-type: none"> • Réception à valider
<ul style="list-style-type: none"> • Outil de simulation de facturation 	<ul style="list-style-type: none"> • Accessibilité de l'outil de simulation de facturation par le CSC 	<ul style="list-style-type: none"> • Outils de simulation accessible par le CSC 24h/24, 7j/7 pendant toute la durée du marché
<ul style="list-style-type: none"> • Outils de pilotage et d'optimisation financière 	<ul style="list-style-type: none"> • Accessibilité des outils de pilotage et d'optimisation financière 	<ul style="list-style-type: none"> • Outils de pilotage et d'optimisation accessible au CSC 24h/24h, 7j/7 pendant toute la durée du marché

2.1.4 PILOTAGE DU SERVICE

PIL-1	Le CSP met à disposition un outil de gestion centralisée des comptes	
<p>Le CSP met à disposition du CSC une solution de gestion centralisée de ses différents comptes sur la plateforme cloud public. Cette gestion doit permettre de contrôler les éléments suivants (non exhaustif) :</p> <ul style="list-style-type: none"> • Les politiques des différents comptes ; • Les droits d'accès aux services et ressources ; • La facturation des différents comptes. 		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outil de gestion des comptes 	<ul style="list-style-type: none"> • Outil à tester par le CSC 	<ul style="list-style-type: none"> • Disponibilité : 24h/24, 7j/7

PIL-2	Le CSP met à disposition des outils de monitoring des services	
<p>Le CSP met à disposition du CSC des outils permettant de connaître en temps réel l'état de ses services. La plateforme de monitoring doit notamment :</p> <ul style="list-style-type: none"> • Alerter en cas de coupure d'un service ou d'une ressource • Alerter en cas de comportement anormal (usage intensif, perte de performance, etc.) d'un service ou d'une ressource) <p>Les outils de monitoring doivent être paramétrés par le CSC (définition de seuils) et permettre de constituer des indicateurs agrégés (disponibilité périodique, etc.).</p> <p>Le CSP met également à disposition les rapports de sécurité de sa plateforme cloud.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outil de monitoring des services 	<ul style="list-style-type: none"> • Outil à tester par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24h/24 et 7j/7
<ul style="list-style-type: none"> • Rapports de sécurité 	<ul style="list-style-type: none"> • Réception des rapports 	<ul style="list-style-type: none"> • Disponibilité 24h/24 et 7j/7

2.1.5 EXIGENCES TECHNIQUES

2.1.5.1 Postes utilisateurs

TEC-1	Les services fonctionnent en client léger (navigateur web)	
<p>Les services doivent fonctionner sur les navigateurs suivants, dans les versions supportées par leurs éditeurs respectifs, pendant toute la durée du marché :</p>		

<ul style="list-style-type: none"> • Firefox ESR • Microsoft Edge • Google Chrome • Safari • ... 	
<i>Contrôle de l'atteinte des résultats :</i> <ul style="list-style-type: none"> • Tests et recette par le CSC 	<i>Niveau à atteindre :</i> <ul style="list-style-type: none"> • Réception à valider

2.1.5.2 IT Network

TEC-2	Le CSP propose des moyens d'interconnexion avec le réseau du CSC	
<p>Le CSP propose des moyens permettant de relier le réseau interne du CSC au réseau de l'infrastructure du CSP.</p> <p>Ces interconnexions doivent permettre :</p> <ul style="list-style-type: none"> ○ L'administration des ressources cloud computing hébergées chez le CSP ; ○ Le transfert des données entre le réseau interne du CSC et l'infrastructure du CSP. <p>Les types d'interconnexion identifiés à ce jour par le CSC (non limitées à d'autres solutions) sont :</p> <ul style="list-style-type: none"> • Liaison Internet du CSC : <ul style="list-style-type: none"> ○ Depuis les clients connectés sur le réseau du CSC vers la solution du CSP (exposition Internet) via les proxys HTTP/HTTPS du CSC ; ○ Depuis les clients connectés sur le réseau du CSC vers la solution du CSP (exposition interne) via l'établissement d'un tunnel VPN IPSec depuis un équipement du CSC vers un équipement fourni par le CSP ; ○ Entre les partenaires externes au CSC et le CSC via la solution de raccordement centralisée des partenaires. • Liaison privée entre le CSC et le responsable du traitement des données : <ul style="list-style-type: none"> ○ Via sa propre infrastructure d'interconnexion ; ○ Via un partenaire du CSP (opérateur) ; ○ Via un centre de colocation (opérateur, plateforme d'échange). • Liaison Internet du CSP. <p>Le CSP doit fournir une solution scalable, sécurisée et hautement disponible pour accéder aux services du CSC depuis Internet.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Liste des moyens d'interconnexion possibles entre le CSP et le CSC 	<ul style="list-style-type: none"> • Documentation à réceptionner par le CSC 	<ul style="list-style-type: none"> • Débit jusqu'à 10Gbps

TEC-3	Les services sont compatibles avec IPv6	
<p>Toutes les communications réseau entre le CSC et le CSP basées sur l'IP se feront nativement en IPv4.</p> <p>Si le CSP souhaite passer à l'IPv6, il doit en faire la demande au CSC, par écrit, un an avant sa mise en œuvre. Le CSP s'engage à conditionner le passage à IPv6 à l'accord formel du CSC. Le CSP fournira une étude des impacts de la migration vers IPv6 sur le service fourni au CSC. Cette étude présentera au moins les éléments architecturaux modifiés ainsi que l'analyse d'impact sur la performance globale du Service.</p> <p>Si le CSC le demande, le CSP devra s'engager à fournir une connexion IPv6. Le CSC devra approuver les nouvelles performances du réseau et la conformité avec la politique de sécurité des SI du CSC après une nouvelle étude et la fourniture de mesures de performance par le CSP du marché.</p> <p>Le CSP s'engage à étudier toute nouvelle fonctionnalité offerte par le protocole IPv6 susceptible d'améliorer le Service fourni au CSC, à la présenter au CSC et à la mettre en œuvre si ce dernier en fait la demande. Le Service doit être pleinement compatible avec le passage à l'IPv6.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Demande de passage à IPv6 du CSP au CSC 	<ul style="list-style-type: none"> • Demande à réceptionner par le CSC 	<ul style="list-style-type: none"> • Réception à valider au moins 1 an avant la date de passage souhaitée par le CSP
<ul style="list-style-type: none"> • Etude d'impacts de la migration en IPv6 sur le SERVICE 	<ul style="list-style-type: none"> • Etude à recevoir par le CSC 	<ul style="list-style-type: none"> • Réception à valider au plus tard 1 mois calendaire après la Demande de passage à IPv6

2.1.5.3 Interopérabilité avec le reste du SI et portabilité

TEC-4	Les services sont accessibles par des APIs	
<p>L'intégralité des services doit pouvoir être adressée par le CSC via des APIs.</p> <p>Dans le cas contraire, le CSP devra en justifier la raison.</p> <p>Le CSP fournit la documentation de ces APIs.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • APIs du catalogue de services du CSP 	<ul style="list-style-type: none"> • Accès aux APIs du catalogue de services du CSP par le CSC 	<ul style="list-style-type: none"> • APIs du catalogue de services du CSP accessibles par le CSC 24h/24, 7j/7 pendant toute la durée du marché.

<ul style="list-style-type: none"> Documentation des APIs du catalogue de services du CSP 	<ul style="list-style-type: none"> Documentation à réceptionner par le CSC 	<ul style="list-style-type: none"> Réception à valider
--	---	---


2.2 PRESTATIONS ATTENDUES

2.2.1 MISE À DISPOSITION DES SERVICES

MES-1	Le CSP met à disposition le catalogue de services	
<p>Le CSP fournit une interface permettant au CSC de s'abonner aux différents services disponibles. Cette interface de catalogue de services, accessible via l'API, doit être différente en fonction des utilisateurs et des droits qui leur sont attribués.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Catalogue de services 	<ul style="list-style-type: none"> Utilisation par le CSC 	<ul style="list-style-type: none"> Disponible 24h/24 et 7j/7

MES-2	Le CSP fournit des tableaux de bord personnalisables	
<p>Le CSP permet au CSC de créer des tableaux de bord personnalisables qui sont visibles lors de la connexion à la plateforme du CSP. Les tableaux de bord servent de page d'accueil à la plateforme, ils présentent les informations et les modules auxquels les utilisateurs veulent accéder rapidement.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Tableaux de bords personnalisables 	<ul style="list-style-type: none"> Utilisation par le CSC 	<ul style="list-style-type: none"> Disponible 24h/24 et 7j/7

2.2.2 RÉVERSIBILITÉ ET PORTABILITÉ

REV-1	Le CSP doit fournir une déclaration de transparence	
	<p>Le CSP d'infrastructure doit fournir une déclaration de transparence en utilisant le modèle [SWIPO cloud IaaS and SaaS services CSP transparency statement version 1.0] et ne doit pas modifier l'ordre et la structure de ce modèle ; cette déclaration de transparence peut être utilisée comme base pour le modèle de contrat.</p> <p>La description dans la déclaration de transparence doit fournir un niveau de détail approprié, y compris :</p> <ul style="list-style-type: none"> Tous les aspects de la conformité à ce code ; 	

- Toute la documentation, le support et les outils disponibles pour transférer les données du CSC d'un CSP d'infrastructure à un autre ;
- une description du processus global de portage des données et des capacités prises en charge, y compris les processus de sauvegarde et de récupération des données adoptés pour protéger les données pendant leur transfert, les mesures de sécurité, la gestion des enregistrements et, s'il en a été convenu ainsi, la suppression des données du CSC après un portage réussi (si le CSC a l'intention de mettre fin à l'accord de services en nuage) si la capacité de suppression est fournie au CSC par le CSP d'infrastructure, le CSC peut procéder lui-même à la suppression. La suppression doit être effectuée par le CSP d'infrastructure source, si cette capacité n'est pas fournie au CSC ;
- Le statut et les procédures de traitement des données du CSC sur l'infrastructure du CSP d'infrastructure après la résiliation, y compris les instructions du CSC concernant toute obligation de conservation, de stockage ou de restauration des données stipulée par la loi ou la réglementation applicable ;
- Une description claire de tous les tiers qui ont accès aux données dans le cadre du processus,
- Une description claire des politiques et des processus d'accès aux données en cas de faillite du CSP d'infrastructure ou d'acquisition par une autre entité. Ces politiques et processus doivent inclure l'information du CSC dans les meilleurs délais dès que la procédure de faillite a été entamée auprès des autorités publiques compétentes ;
- Si un prestataire de services tiers est nécessaire pour convertir, traduire ou transférer les artefacts d'infrastructure du CSC, cela doit être explicitement indiqué dans la déclaration de transparence du CSC ;
- L'étendue des artefacts d'infrastructure disponibles pour le transfert ;
- Toute revendication de droits de propriété intellectuelle que le fournisseur de services d'infrastructure détient sur les données du CSC, et la manière dont ces droits sont appliqués après un basculement.

Avant que le CSC n'accepte le contrat de service (CSA), le CSP d'infrastructure doit fournir au CSC une déclaration de transparence décrivant les mécanismes liés au portage des données du CSC :

- des installations sur site du CSC vers le service cloud du CSP d'infrastructure ;
- d'un autre service cloud vers un service cloud du CSP d'infrastructure ;
- et pour les installations sur site du CSC (du service cloud du CSP d'infrastructure) vers un autre service cloud du CSP d'infrastructure, s'ils s'appliquent aux données du CSC, et comment ces aspects sont pris en compte lors de l'examen de la portabilité des données.
- Il devra également décrire l'ensemble des domaines de coût connexe qui serait facturé par le CSP d'infrastructure.


Il doit veiller à ce que les informations relatives à la portabilité des données soient mises à la disposition du CSC, y compris en ligne et/ou incorporées par référence dans d'autres documents contractuels, et à ce que ces informations soient tenues à jour.


Le CSP de l'infrastructure informe le CSC périodiquement et en temps utile de toute modification des mécanismes et des conditions, y compris des coûts identifiés, qui modifierait de manière significative la portabilité des données du CSC. Le CSC doit avoir le droit de résilier l'accord à l'avance.


Le CSP d'infrastructure informe périodiquement et sans retard injustifié le CSC de toute modification permanente de sa déclaration d'adhésion au document de référence.

Il est à noter que la mise à disposition des informations précontractuelles aux CSC potentiels ne nécessite pas une divulgation publique et peut se faire sur une base confidentielle (par exemple via un accord de non-divulgence (NDA)).

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Déclaration de transparence du CSP 	<ul style="list-style-type: none"> • Documentation à réceptionner par le CSC 	<ul style="list-style-type: none"> • Réception à valider

REV-2	Le CSP permet au CSC de récupérer ses données	
		
<p>Le CSC doit pouvoir gérer la réversibilité des services fournis par le CSP vers d'autres services d'un tiers ou du CSC. La réversibilité ne s'applique pas aux architectures mises en œuvre dans les infrastructures du CSP mais concerne les données qui y sont hébergées.</p> <p>Le CSP doit permettre au CSC de récupérer l'ensemble de ses données. Le CSC est responsable du transfert des données. Le CSP s'assure que les sources de données sont utilisables par le CSC.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Documentations sur la réversibilité 	<ul style="list-style-type: none"> • Le CSC récupère toutes ses données 	<ul style="list-style-type: none"> • Aucune perte de donnée

REV-3	Le CSP efface les données après leur récupération par le CSC.	
		
<p>Une fois les données récupérées par le CSC, et après accord du CSC, le CSP s'engage à supprimer de manière sécurisée toutes les données traitées par les services.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Procédure d'effacement des données 	<ul style="list-style-type: none"> • Caractère complet de l'effacement des données • Délai d'effacement des données 	<ul style="list-style-type: none"> • Toutes les données à supprimer ont été supprimées au plus tard 10 jours ouvrables après le consentement du CSC.

<p>REV-4</p> 	<p>Le CSP doit préciser tous les processus qu'il prend en charge pour maintenir l'intégrité des données, la continuité des services et la prévention des pertes de données spécifiques à l'exportation de données.</p>	
<p>Le CSP doit décrire tous les processus qu'il prend en charge pour maintenir l'intégrité des données, la continuité des services et la prévention des pertes de données spécifiques à l'exportation de données. Cela comprend la sauvegarde et la vérification des données avant et après le transfert, la gestion des temps d'arrêt et la transmission sécurisée, la fonctionnalité de retour en arrière et toute fonctionnalité de test.</p> <p>Le CSP doit également détailler toutes les données d'audit de sécurité, telles que les journaux d'accès, qui sont disponibles pour l'exportation. Ces journaux des interactions des utilisateurs avec le service en nuage peuvent être nécessaires pour l'analyse de la sécurité et pour les demandes de contrôle.</p> <p>Le cas échéant, le CSP doit préciser les processus et services de chiffrement fournis lors de l'exportation des données, y compris les options non chiffrées. Il doit décrire comment les clés de chiffrement sont gérées pour permettre au CSC de déchiffrer les données exportées.</p> <p>Enfin, le CSP doit préciser les contrôles de sécurité, tels que les contrôles d'accès, disponibles lors de l'exportation des données.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> Description des processus de sécurité pour l'exportation des données 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation des documents par le CSC

<p>REV-5</p>	<p>Le CSP doit spécifier le processus explicite et structuré pour l'importation de données.</p>	
<p>Le CSP doit définir un processus clair et structuré pour l'importation des données. Ce processus doit inclure des considérations relatives à la gestion des données, telles que les instantanés et les approches par étapes, les politiques de gestion des enregistrements et l'évaluation de la bande passante. Il doit également détailler tous les délais pertinents, les exigences en matière de notification, les procédures de contact avec les clients et l'impact sur la continuité du service. Le processus et la documentation doivent couvrir les questions techniques, contractuelles et de licence de manière suffisante pour permettre le portage et le basculement.</p> <p>Le CSP doit également détailler tous les outils nécessaires qui entraînent des coûts supplémentaires pour l'importation de données. Il doit préciser tous les outils ou services fournis, y compris le soutien à l'intégration ou à l'interopérabilité, qui sont disponibles pour faciliter le processus d'importation, ainsi que les coûts associés à ces outils. Tous les outils ou services de tiers doivent être précisés.</p> <p>Le CSP doit préciser si le client peut être totalement indépendant dans l'importation des données, c'est-à-dire lorsque le client du service cloud n'a pas besoin d'interaction humaine avec le fournisseur. Il doit préciser quelles données, y compris les données dérivées d'un service</p>		


d'exportation source telles que les valeurs de champ calculées, les graphiques, les affichages, peuvent être importées dans le service.


Le CSP doit détailler le format/la structure requis des données importées et indiquer où les définitions sont disponibles et sous quelles conditions. Cela inclut les formats industriels ou open source tels que le format Open Financial Exchange. Le fournisseur doit préciser tous les validateurs disponibles et, le cas échéant, leur type, leur provenance et les conditions dans lesquelles ils sont utilisés. Ces informations doivent être suffisantes pour permettre le portage et la commutation.


Le CSP doit spécifier la structure des coûts pour l'importation des données et les procédures associées, telles que les restrictions de volume. Il peut spécifier tout service de migration supplémentaire existant, qu'il soit fourni par le CSP ou par une tierce partie, et la manière dont il est disponible sur le marché.

Le CSP doit préciser toute obligation imposée avant le début de l'importation des données. Il doit préciser les processus de chiffrement utilisés lors de l'importation de données, y compris les options non chiffrées, et la manière dont les clés de chiffrement sont gérées.


Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Procédures d'importation, y compris les coûts et les outils 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC


REV-6	Le CSP utilise un format standard pour sa structure de données	
		
<p>Le CSP doit préciser les normes de données, les formats et/ou les types de fichiers recommandés, utilisés ou disponibles pour l'importation et l'exportation de données (par exemple, binaire, MIME, CSV, SQL, JSON, XML, Avro) pour chaque ensemble de données disponible à l'importation, y compris les données non structurées.</p> <p>Le CSP doit fournir une documentation sur le format et la structure des données exportées, y compris leur provenance, et dans quelles conditions, si elles proviennent d'un tiers (y compris les formats de l'industrie ou open source (par exemple le format Open Financial Exchange)). Cette documentation doit être suffisante pour permettre le portage et la commutation.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Documentation sur la structure des données et les utilisations standard 	<ul style="list-style-type: none"> Validation par le CSC 	<ul style="list-style-type: none"> Le CSP doit veiller à ce que les normes de données soient basées sur des normes standards du marché.

REV-7 	Le CSP fournit une solution de portabilité au CSC	
<p>Le CSP doit fournir au CSC les procédures (et les services) permettant d'initier le basculement et le portage à partir du service en nuage lorsque celui-ci est une source de portage.</p> <p>Le CSP doit informer le CSC des éléments suivants :</p> <ul style="list-style-type: none"> • les conditions disponibles pour le basculement et le portage vers le service cloud ; • les méthodes et formats de portage disponibles ; • les frais et les conditions associés aux services de portage. Les frais et les conditions doivent être clairement affichés au stade de l'abonnement, avec des mécanismes d'avertissement qui informent le CSC de sa capacité à utiliser les services de réversibilité après une phase d'engagement. <p>Le transfert d'artefacts d'infrastructure du CSC vers et depuis le service cloud doit utiliser des normes et des protocoles ouverts pour le mouvement des artefacts d'infrastructure.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Procédure de portage • Conditions de portage et de commutation. • Frais et conditions des services de portage 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

REV-8 	Le CSP fournit une procédure de portage dans le cas où le CSC souhaite la cessation d'un service	
<p>Le CSP doit fournir au CSC un processus de sortie d'un service cloud existant, lorsqu'il est la source du portage, et que le CSC vise à mettre fin à son utilisation du service cloud une fois le portage terminé. Ce processus doit être accompagné d'une matrice de portage sur l'étendue des services cibles et la destination du processus de portage.</p> <p>Le CSP doit préciser la période, définie et négociée au moment de l'activation du processus de portabilité, pendant laquelle les données du CSC resteront disponibles pour le transfert une fois que la résiliation du service source est demandée par le CSC, ainsi que la nature des avertissements clairs et opportuns émis avant la suppression des données du CSC.</p> <p>Les coûts de la procédure de portage doivent être explicites avant la signature de tout contrat et doivent être conformes à l'article 29 de la loi sur les données jusqu'à leur disparition complète.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Matrice de portage 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC


<ul style="list-style-type: none"> Procédure de résolution 		
<u>Niveau de confiance (BONUS)</u> : Le CSP doit fournir au CSC les méthodes et formats de portage normalisés, documentés, certifiés et sécurisés disponibles, y compris les garanties disponibles et les restrictions et limitations techniques connues.	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC
<u>Niveau de confiance (BONUS)</u> : Le CSP doit fournir au CSC les capacités de gestion nécessaires au processus de portage et de commutation (par exemple, gestion de bout en bout pour éviter la perte de service pour le client).	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

REV-9 	Le CSP doit fournir au CSC des procédures de commutation et de portage pour l'activation d'un nouveau service cloud lorsqu'il est la destination du portage.	
<p>Le CSP doit fournir au CSC des procédures de commutation et de portage pour l'activation d'un nouveau service en nuage lorsqu'il est la destination de portage.</p> <p>(Lorsque le CSP est une destination de portage, il doit fournir les procédures permettant de lancer le service avec les données récupérées par le CSC auprès d'un CSP précédent).</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Procédure d'activation du service cloud 	<ul style="list-style-type: none"> Réception of the documents by the CSP 	<u>Niveau de confiance requis</u> : Le CSP doit fournir au CSC (les services et) les procédures pour initier la commutation et le portage d'un service cloud vers la nouvelle destination.

<p>REV-10</p> 	<p>Le CSP doit permettre l'importation et l'exportation des artefacts d'infrastructure CSC.</p>	
<p>Le CSC doit pouvoir importer et exporter les artefacts d'infrastructure CSC de manière simple et sécurisée, en prenant en charge les scénarios suivants :</p> <ul style="list-style-type: none"> • CSC vers service cloud ; • Service cloud vers service cloud ; • Service cloud vers CSC. <p>L'infrastructure CSP fournira les moyens permettant le transfert en utilisant un format structuré, couramment utilisé et lisible par les machines. Ces moyens doivent être documentés pour les différents scénarios.</p> <p>L'infrastructure CSP doit fournir la procédure permettant au CSC de tester les mécanismes de transfert et de convenir d'un calendrier de transfert, en fonction des besoins de son unité commerciale et des risques de sécurité. La procédure doit également spécifier les moyens pouvant être fournis par le CSP en termes de support. Les tests de transfert doivent inclure à la fois les tests des mécanismes utilisés pour importer et exporter des données vers et depuis un service cloud, ainsi que les API utilisées pour accéder et gérer les données lorsqu'elles sont stockées dans le service cloud. Les tests doivent être acceptés par le CSC, dans le cadre d'un processus de test transparent. Le CSC doit être conseillé par l'infrastructure CSP sur les besoins supplémentaires en matière de tests.</p> <p>Lorsque les données du CSC impliquent des artefacts d'infrastructure qui reposent sur une fonctionnalité ou une capacité d'un service cloud, le CSP doit fournir une description appropriée de l'environnement pour leur exécution et comment les dépendances de service peuvent être atteintes. Une matrice d'impact de la portabilité doit indiquer les dépendances à prendre en compte lors de la portabilité.</p> <p>Le CSP doit mettre à la disposition du CSC les procédures opérationnelles pour transférer leurs données une fois que la résolution du service source est demandée par le CSC.</p> <p>Pour le volume attendu d'Artefacts d'Infrastructure, l'infrastructure CSP doit fournir les mécanismes appropriés, les périodes de disponibilité et le prix de transfert. Ces éléments doivent être affichés, connus et acceptés par le CSC dès que le CSC signe le contrat avec le CSP.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Documentation pour chaque scénario • Procédure des mécanismes de transfert • Matrice de portabilité • Procédure opérationnelle de transfert 	<ul style="list-style-type: none"> • Réception des documents et des tests de la part du CSP 	<ul style="list-style-type: none"> • Validation des documents par le CSP <p><u>Niveau de confiance requis :</u> Le CSP d'infrastructure doit prendre des mesures raisonnables, minimisant l'impact sur la qualité du service, pour permettre au CSC de maintenir la</p>

		continuité du service lors du transfert de données entre fournisseurs, lorsque cela est techniquement possible.
--	--	---


REV-11	Le CSP doit informer le CSC du calendrier de migration des données.	
<p>Le CSP doit informer le CSC du calendrier de migration des données. Il doit fournir la période pendant laquelle les données CSC resteront disponibles pour le transfert une fois que la résiliation du service source est demandée par le CSC, ainsi que la nature des avertissements clairs et opportuns émis avant la suppression des données CSC.</p> <p>Ces éléments doivent être affichés, connus et acceptés par le CSC dès que le CSC signe le contrat avec le CSP.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Calendrier de migration des données 	<ul style="list-style-type: none"> Réception des documents par le CSP 	<p><u>Niveau de confiance requis :</u></p> <p>L'infrastructure CSP doit fournir un calendrier de migration des données, intégré à des rapports de portabilité avec une durée contractée à l'avance, en utilisant les meilleures pratiques actuelles et les technologies disponibles, y compris des solutions non connectées, afin d'avoir une vue d'ensemble globale des opérations de bout en bout.</p>


REV-12	Le CSP veille à ce que des pratiques soient en place pour faciliter le changement de prestataires de services.	
		
<p>Le CSP doit s'assurer que des pratiques sont en place pour faciliter le changement de prestataires de services et le transfert de données dans un format structuré, couramment utilisé et lisible par les machines, incluant les formats standard ouverts lorsque requis ou demandés par le prestataire de services recevant les données. Ces éléments doivent être incorporés dans le modèle contractuel du CSC.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Description de différents 	<ul style="list-style-type: none"> Résultat du suivi Réception des documents par le CSP 	<ul style="list-style-type: none"> Validation par le CSC

REV-13	Le CSP veille à ce qu'il y ait des informations précontractuelles disponibles sur la portabilité des données	
Le CSP doit veiller à ce que des informations précontractuelles soient disponibles, avec des informations suffisamment détaillées, claires et transparentes sur les processus de portabilité des données, les exigences techniques, les délais et les frais en cas de souhait de l'utilisateur professionnel de passer à un autre prestataire de services ou de transférer des données vers ses propres systèmes informatiques. Ces éléments doivent être incorporés dans le modèle contractuel du CSC.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Informations précontractuelles sur la portabilité (peut être un lien vers un site web) 	<ul style="list-style-type: none"> Monitoring results: Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

REV-14	Le CSP doit fournir une FAQ au CSC concernant l'exportation d'informations sur les artefacts.	
Lors de l'exportation d'artefacts du CSC vers un service cloud, ou entre services cloud, le CSP doit fournir une FAQ au CSC comprenant des éléments pour l'utilisateur, l'administrateur et les fonctions commerciales et métiers, liées au service cloud.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> FAQ concernant la portabilité (peut être un lien vers un site web) 	<ul style="list-style-type: none"> Monitoring results Reception of the documents by the CSP 	<ul style="list-style-type: none"> Validation par le CSC
<u>Niveau de confiance (BONUS) :</u> Lors de l'exportation d'artefacts du CSC vers un service cloud, ou entre services cloud, le CSP doit fournir un support pour faciliter l'interopérabilité entre les capacités du CSC, y compris les fonctions utilisateur, administrateur et commerciales liées au service cloud.	<ul style="list-style-type: none"> Reception of the documents by the CSP 	<ul style="list-style-type: none"> Validation par le CSC
<u>Niveau de confiance (BONUS) :</u> Le CSP doit déclarer tout support facilitant l'interopérabilité entre les capacités du CSC, y	<ul style="list-style-type: none"> Reception of the documents by the CSP 	<ul style="list-style-type: none"> Validation par le CSC

compris les fonctions utilisateur, administrateur et commerciales liées au service cloud.		
---	--	--

REV-15 	Le CSP doit garantir la réversibilité des données en utilisant les méthodes techniques à sa disposition.	
<p>Le CSP doit garantir la réversibilité des données en utilisant les méthodes techniques à sa disposition.</p> <p>Les détails techniques de la réversibilité sont définis dans l'accord de service. Ces éléments doivent être intégrés dans le modèle contractuel du CSC.</p> <p>Le CSP doit préciser la bande passante disponible et le temps estimé pour la récupération de toutes les données du CSC.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Engagement du CSP et informations sur le processus de récupération 	<ul style="list-style-type: none"> Monitoring results Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC
<p><u>Niveau de confiance (BONUS) :</u></p> <p>Le CSP doit garantir cette réversibilité grâce à l'une des méthodes techniques suivantes :</p> <ul style="list-style-type: none"> La fourniture de fichiers dans un ou plusieurs formats documentés pouvant être utilisés en dehors du service fourni par le prestataire de services ; La mise en œuvre d'interfaces techniques permettant l'accès aux données via un plan documenté et utilisable (API, format pivot, etc.). 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

REV-16 	Le CSP doit spécifier le processus explicite et structuré pour l'exportation des données.	
<p>Le CSP doit décrire un processus clair et structuré pour l'exportation des données. Ce processus devrait inclure des considérations pour la gestion des données, telles que les instantanés et les approches par phases, les politiques de gestion des enregistrements et l'évaluation de la bande passante. Il devrait également détailler tous les délais pertinents, les exigences de notification, les procédures de contact avec le client et l'impact sur la continuité du service. La disponibilité du processus d'exportation des données pendant et après la période contractuelle, ainsi que les SLO et SQO du SLA, doivent être inclus. Le processus et la documentation doivent couvrir suffisamment les questions techniques, contractuelles et de licence pour permettre le portage et le changement.</p> <p>Avant que l'exportation des données ne puisse commencer, le CSP doit spécifier contractuellement toutes les obligations. Il doit également détailler tous les frais de licence post-contractuels connus ou autres engagements, tels que les redevances de brevet et de licence couvrant l'utilisation de données dérivées ou de formats de données ou les réclamations et cas en attente. Ces éléments doivent être ajoutés à la matrice d'impact.</p> <p>Le CSP doit détailler tout outil et service entraînant des coûts supplémentaires pour l'exportation de données requise par les processus du fournisseur source pour la portabilité des données et fournir une mise à jour continue de ces outils et services. Ces éléments doivent également être ajoutés à la matrice d'impact. Il doit spécifier tous les outils ou services fournis, y compris le support pour l'intégration ou l'interopérabilité, qui sont disponibles pour aider le processus d'exportation, ainsi que les coûts associés à ces outils. Tous les outils ou services tiers doivent être spécifiés dans un catalogue de portabilité.</p> <p>Le CSP doit informer le CSC de ses processus de portabilité des données et indiquer le degré d'autonomie du CSC lors de l'exportation. Il doit spécifier quelles données, y compris les données dérivées telles que les valeurs de champs calculées, les graphiques, les affichages, peuvent être exportées du service avant la date effective d'exportation.</p> <p>Le CSP doit détailler la structure des coûts pour l'exportation des données et les procédures associées. Il doit fournir une transparence suffisante pour permettre au client du service cloud de calculer toutes les charges d'exportation de données imposées par le fournisseur. Le CSP doit produire une matrice de réversibilité et spécifier les dépendances connues entre les données à exporter et d'autres données connectées à un autre service cloud.</p> <p>Enfin, le CSP doit spécifier les mécanismes, protocoles et interfaces disponibles pouvant être utilisés pour effectuer l'exportation des données, tels que VPN LAN à LAN, Data Power, SFTP, HTTPS, API, support physique, etc.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Procédures de réversibilité incluant les coûts et les outils 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Validation des documents par le CSC

<ul style="list-style-type: none"> • Matrice de réversibilité • Matrice d'impact 		
<p><u>Niveau de confiance (BONUS)</u>: Le CSP doit indiquer si ses processus sources pour la portabilité des données permettent au CSC d'être totalement indépendant lors de l'exportation des données, c'est-à-dire lorsque le client n'a pas besoin d'interaction humaine avec le fournisseur.</p>		

REV-17	Le CSP d'infrastructure doit fournir des API liées à la portabilité des services cloud.	
<p>Le CSP d'infrastructure doit fournir des API liées à la portabilité des services cloud, et si elles sont fournies, elles doivent être entièrement documentées. Un catalogue des API de transfert partagées doit être mis à la disposition du CSC par le CSP. Ces API doivent permettre le transfert d'artefacts d'infrastructure entre les parties participantes. Si des bibliothèques de code ou des dépendances associées existent, elles doivent être documentées et mises à disposition.</p> <p>Le CSP doit informer le CSC de l'existence d'une interface lui permettant d'effectuer des extractions de données.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • API de portabilité • Catalogue d'API de transfert partagé 	<ul style="list-style-type: none"> • Monitoring results • Réception des documents et tests par le CSC 	<ul style="list-style-type: none"> • CSC validation
<p><u>Niveau de confiance (BONUS)</u>: Le CSP d'infrastructure doit fournir une interface en libre-service permettant au CSC d'effectuer des extractions de données périodiques à partir du CSC. Cette fonctionnalité peut être contractée et peut entraîner des coûts supplémentaires. L'opérabilité de la réversibilité doit être démontrée et vérifiée par le biais de processus de surveillance périodiques et à l'initiative du CSC.</p>	<ul style="list-style-type: none"> • Réception des documents et tests par le CSC 	<ul style="list-style-type: none"> • CSC validation

2.2.3 MARKET PLACE

MAR-1	Le CSP met à disposition sa <i>Market Place</i>	
<p>Le CSP met à disposition du CSC les services d'éditeurs tierces accessibles via sa <i>Market Place</i> tels que :</p> <ul style="list-style-type: none"> • Les services DevOps ; • Les services Business apps ; • Les services de migration ; • Les services de stockage ; • Les services réseaux ; • Les services de sécurité ; • Les services de bases de données. 		
Livvable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Services de la <i>Market Place</i> 	<ul style="list-style-type: none"> • Accessibilité à la <i>Market Place</i> 	<ul style="list-style-type: none"> • Accessible 24h/24, 7j/7

MAR-2	Le CSP met à disposition une <i>Market Place</i> privée	
<p>Le CSP met à disposition du CSC les services d'une <i>Market Place</i> privée, qui lui permet de filtrer l'accès et les produits qu'elle met à disposition.</p>		
Livvable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Services de la <i>Market Place</i> privée 	<ul style="list-style-type: none"> • Accessibilité à la <i>Market Place</i> privée 	<ul style="list-style-type: none"> • Accessible 24h/24, 7j/7

2.2.4 CONSTRUCTION DU SOCLE D'INFRASTRUCTURE

CONS-01	Le CSP met en place le socle d'infrastructures cloud public
<p>Le CSP met en place le socle d'infrastructures cloud public du CSC.</p> <p>Le CSP précisera le délai et les coûts associés ainsi que les prérequis.</p> <p>Lister les services du Socle :</p> <p><u>Gestion des accès et identités :</u></p> <ul style="list-style-type: none"> • Service de gestion des identités et des accès (IAM) ; • Service d'authentification unique ; • Service d'annuaire ; • Service de gestion centralisée des comptes ; • Service de gestion des Secrets ; • Service de partage des ressources. 	

Détection des incidents :

- Service pour afficher et gérer de manière centralisée les alertes de sécurité et automatiser les contrôles de conformité ;
- Service de détection intelligente des menaces et surveillance continue pour protéger les comptes et les charges de travail ;
- Service pour enregistrer et évaluer les configurations des ressources pour permettre l'audit de conformité, le suivi des modifications des ressources et l'analyse de la sécurité ;
- Service pour suivre l'activité des utilisateurs et l'utilisation des API pour permettre la gouvernance, la conformité et l'audit opérationnel / des risques du compte ;
- Service de visibilité complète des ressources et applications cloud pour collecter des métriques, surveiller les fichiers journaux, définir des alarmes et réagir automatiquement aux changements ;
- Service pour capturer des informations sur le trafic IP entrant et sortant des interfaces réseau dans du VPC du CSC.

Protection des infrastructures :

- Service pour configurer et gérer les systèmes locaux pour appliquer des correctifs de système d'exploitation, créer des images système sécurisées et configurer des systèmes d'exploitation sécurisés ;
- Service de protection DDoS qui protège les applications Web exécutées ;
- Service Web Application Firewall pour protéger les applications Web contre les failles Web courantes et garantir la disponibilité et la sécurité de vos services ;
- Service de gestion des Firewall pour configurer et gérer de manière centralisée les règles WAF sur les comptes et les applications ;
- Service pour automatiser les évaluations de sécurité pour améliorer la sécurité et la conformité des applications déployées ;
- Service de *Virtual Private* cloud (VPC) pour provisionner une section isolée logiquement du cloud du CSP depuis laquelle le CSC peut lancer des ressources du CSP dans un réseau virtuel défini par le CSC

Protection des données :

- Service de gestion des clés de chiffrement pour créer et contrôler facilement les clés utilisées pour chiffrer les données ;
- Service de chiffrement des données (cloud HSM) ;
- Service de gestion des certificats pour gérer et déployer facilement des certificats SSL / TLS ;
- Service d'options de chiffrement des données flexibles à l'aide de clés gérées par le CSP, de clés ou de clés gérées par le CSP.

Réponses aux incidents :

- Services de Config Rules pour créer des règles qui prennent automatiquement des mesures en réponse aux changements dans l'environnement du CSC, comme isoler des ressources, enrichir des événements avec des données supplémentaires ou restaurer la configuration à un état connu.


Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Service implémenté et configuré sur base des spécifications du CSC • Script de déploiement et de configuration en infra as code et Terraform préconisé 	<ul style="list-style-type: none"> • Validé par le CSC 	<ul style="list-style-type: none"> • Validé par le CSC


2.3 PILOTAGE DES SERVICES CONCERNANT L'OPERATIONAL READINESS

2.3.1 GESTION DE LA DISPONIBILITÉ DES SERVICES

PRD-1	Les services sont disponibles sur une plage de service garantie	
<p>Le CSP garantit la disponibilité du Service, vue de son point de sortie sur l'Internet.</p> <p>La méthode de calcul du taux de disponibilité est la suivante :</p> <ul style="list-style-type: none"> • Taux de disponibilité (en %) = $100 \times (1 - (\text{Nombre d'heures d'indisponibilité du parcours de test dans la période donnée} / \text{Nombre d'heures dans la période donnée}))$ • La base de calcul est de 24 heures/jour et de 720 heures par mois (30 jours). <p>LE CSC pourra effectuer ses propres mesures de disponibilité du Service via une solution tierce de supervision applicative, interopérable avec le cloud du CSP.</p> <p>L'ensemble des articles du catalogue de services du CSP est disponible sur une plage de service garantie : 24h/24, 7j/7.</p> <p>Dans le cas contraire, le CSP devra en justifier la raison pour les services concernés.</p> <p>Le CSP s'engage à respecter les taux de disponibilité des services de son catalogue tels que publiés au CSC. Il s'engage à verser des compensations financières dès la perte de disponibilité. Ces compensations pourront être graduelles en fonction des indisponibilités mesurées. En Annexe sont précisés les engagements de disponibilité et compensations en cas de perte de disponibilité sur les services exigés au CCTP.</p> <p>LE CSC bénéficie de cette compensation financière sous forme de crédits en € pouvant être utilisés pour acheter les services au catalogue du CSP.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Absence d'arrêt et d'incidents sur les services 	<ul style="list-style-type: none"> • Utilisation des services par le CSC sur les plages de service prévues 	<ul style="list-style-type: none"> • Tous les services sont disponibles pendant les périodes définies de la plage de service

2.3.2 GESTION DE LA CONTINUITÉ DU SERVICE

PRD-2		Le CSP garantit la continuité du SERVICE	
			
<p>En cas de survenue d'un désastre ou d'un incident majeur survenant sur le site nominal où le SERVICE est hébergé, le CSP garantit la reprise du Service sur un site de sauvegarde distant.</p> <p>Le CSP doit documenter et mettre en œuvre des procédures pour maintenir ou restaurer le fonctionnement du SERVICE et assurer la disponibilité des informations au niveau et dans le délai auquel le CSP s'est engagé auprès du CSC dans l'accord de service.</p> <p>Le CSP doit documenter et mettre en œuvre des mesures pour répondre à l'exigence de disponibilité du service définie dans la CSA.</p> <p>Le CSP doit indiquer les mesures mises en place pour faire face à une situation d'interruption de service.</p> <p>Dans le déroulement d'un tel incident, le CSP doit réaliser les activités suivantes :</p> <ul style="list-style-type: none"> • Communiquer au CSC sur l'avancement de la reprise d'activité ; • Tester le bon fonctionnement du Service une fois rétabli sur l'environnement de secours en collaboration avec le CSC ; • Re-localiser dès que possible le Service sur son site nominal d'hébergement ; • Faire un retour d'expérience de l'incident et mettre en place un plan d'actions d'améliorations ou de correction d'incidents. 			
Livvable(s) :		Contrôle des résultats :	
<ul style="list-style-type: none"> • Plan de Reprise d'Activités 		<ul style="list-style-type: none"> • Délai de reprise d'activité 	
<ul style="list-style-type: none"> • Retour d'expérience et plan d'actions 		<ul style="list-style-type: none"> • Réception du retour d'expérience 	
		<ul style="list-style-type: none"> • Reprise sous un délai de 1 jour ouvré maximum 	
		<ul style="list-style-type: none"> • Retour d'expérience reçu au plus tard 10 jours ouvrés après le déroulement du PRA 	

PRD-3		Le CSP doit garantir une autonomie continue pour tout ou partie des services qu'il fournit.	
			
<p>Le CSP doit garantir une autonomie continue pour tout ou partie des services qu'il fournit. Le concept d'autonomie opérationnelle doit être compris comme la capacité à maintenir la fourniture du services cloud en s'appuyant sur les compétences propres du fournisseur ou en utilisant des alternatives adéquates.</p>			

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Plan de Reprise d'Activités 	<ul style="list-style-type: none"> Délai de reprise d'activité 	<ul style="list-style-type: none"> Reprise sous un délai de 1 jour ouvré maximum

2.3.3 GESTION DE LA PERFORMANCE DU SERVICE

PRD-4	Les services effectuent des traitements de haute performance	
<p>Toutes les demandes d'éléments du catalogue de services du CSP sont prises en compte et exécutées dans les délais suivants :</p> <p>Niveau d'attente spécifique : Demandes traitées en moins de 5 minutes.</p> <p>Dans le cas contraire, le CSP devra justifier la raison des services concernés.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Performance des services : Exécution réussie des demandes vers le catalogue de services dans les délais spécifiés 	<ul style="list-style-type: none"> Sinon, le CSP devra justifier la raison des services concernés Utilisation du SERVICE par le CSC 	<ul style="list-style-type: none"> Taux de réalisation des demandes dans les délais > 99%

2.3.4 ÉVOLUTION DU SERVICE

PRD-5	Le CSP permet au SERVICE d'évoluer.
<p>Le CSC bénéficie, dans le cadre du contrat, de la fourniture de nouvelles versions et mises à jour des services ainsi que des paramètres associés aux nouvelles fonctionnalités incorporées dans ces nouvelles versions et mises à jour. Une évolution peut être soit l'ajout d'un service au catalogue, soit une mise à niveau de version (à l'exclusion des correctifs de sécurité ou des correctifs de bugs) d'un service existant dans le catalogue, soit la suppression d'un service existant dans le catalogue.</p> <p>Le CSP notifie au CSC les modifications apportées à son catalogue de services (date, nature, impact sur le SERVICE existant) avant tout changement.</p> <p>Le CSP doit mettre à jour le Service pour prendre en compte les changements légaux et réglementaires ayant un impact sur les services et le CSC.</p> <p>Le CSP garantit l'absence de régression fonctionnelle et technique suite aux mises à niveau de version et mises à jour effectuées sur le Service. Il assure également la compatibilité ascendante des versions.</p> <p>Le CSP fournit une description détaillée du contenu de toute nouvelle version. Il fournit une justification détaillant les raisons fonctionnelles ou techniques derrière la mise à niveau.</p>	

Le CSP fournit la documentation technique et fonctionnelle des nouvelles versions et mises à jour nécessaires à l'utilisation du Service : guide de l'utilisateur, guide de l'administrateur, notes de version, etc.


En cas de suppression d'un service existant dans le catalogue, le CSP doit convenir avec le CSC d'un calendrier des étapes de suppression.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Notification au CSC des changements du catalogue de services 	<ul style="list-style-type: none"> Date limite de notification 	<ul style="list-style-type: none"> Échéancier convenu avec le CSC pour la suppression des services du catalogue
<ul style="list-style-type: none"> Documentation des services : guide de l'utilisateur, guide de l'administrateur, notes de version, etc. 	<ul style="list-style-type: none"> Délai de livraison pour les mises à niveau 	<ul style="list-style-type: none"> Selon le calendrier convenu avec le CSC

2.3.5 SUPPORT

PRD-6	Le CSP assure le support aux utilisateurs du Service									
<p>Le CSP doit assurer un support aux utilisateurs du Service. La plage horaire du support doit correspondre à celle du service souscrit.</p> <p>Ce support doit être joignable par téléphone ou par mail et faire dans tous les cas l'objet d'une trace écrite.</p> <p>Les demandes de support relatives à des incidents doivent être traitées en gestion des incidents.</p> <p>Les demandes de support relatives à des anomalies doivent être traitées en gestion des anomalies.</p> <p>Les autres demandes consistent en des demandes d'informations.</p> <p>Les sollicitations de support doivent faire l'objet d'une réponse dans les délais suivant selon la gravité :</p>										
<table border="1"> <thead> <tr> <th>Criticité de l'incident</th> <th>Délai de réponse</th> </tr> </thead> <tbody> <tr> <td>Bloquant</td> <td>Inférieur à 1 heure</td> </tr> <tr> <td>Majeur</td> <td>Inférieur à 4h</td> </tr> <tr> <td>Mineur</td> <td>Inférieur à 12h</td> </tr> </tbody> </table>			Criticité de l'incident	Délai de réponse	Bloquant	Inférieur à 1 heure	Majeur	Inférieur à 4h	Mineur	Inférieur à 12h
Criticité de l'incident	Délai de réponse									
Bloquant	Inférieur à 1 heure									
Majeur	Inférieur à 4h									
Mineur	Inférieur à 12h									
<p>Les demandes d'informations doivent faire l'objet d'une réponse dans un délai inférieur à 24h.</p> <p>Le CSP produit un reporting mensuel sur les demandes de support.</p>										
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :								
<ul style="list-style-type: none"> Réponses aux demandes de support 	<ul style="list-style-type: none"> Disponibilité du support 	<ul style="list-style-type: none"> 100% des sollicitations doivent faire l'objet 								

	<ul style="list-style-type: none"> Délai de traitement des demandes d'informations. 	d'une réponse selon le tableau ci-dessus
<ul style="list-style-type: none"> Reporting sur les demandes de support 	<ul style="list-style-type: none"> Délai de fourniture du reporting 	<ul style="list-style-type: none"> Reporting du mois

PRD-7 	Le support est assuré en français	
<p>Le support est assuré en français.</p> <p>Lorsque le support ne peut pas être assuré en français mais en anglais seulement, le CSP explicite les raisons de cette absence de support en français.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Service de support 	<ul style="list-style-type: none"> Recours au support par le CSC 	<ul style="list-style-type: none"> Disponibilité du support dans les langues spécifiées ci-dessus

PRD-8	Les services du CSP disposent d'une aide en ligne	
<p>Les services doivent disposer d'une aide en ligne en français ou en anglais.</p> <p>Cette aide en ligne doit prendre au minimum les formes suivantes : documentation des services, tutoriels (Guide Utilisateur, Guide Administrateur).</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Aide en ligne adaptée à la version en cours du catalogue de services du CSP 	<ul style="list-style-type: none"> Consultation de l'aide en ligne par le CSC 	<ul style="list-style-type: none"> Aide en ligne mise à jour et accessible 24h/24, 7j/7 pendant toute la durée du marché

PRD-9	Le CSP met à disposition une assistance technique d'architecture pour le « prototypage » des projets	
<p>Le CSP met à disposition une assistance technique d'architecture pour le « prototypage » des projets. Il s'agit d'une assistance aux projets pour bien démarrer dans le cloud public, se faire une idée de la conception et des coûts associés à un prototype d'architecture (« High Level Design »). L'assistance technique livre un schéma d'architecture et une cotation de cette architecture.</p>		


Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Prototype d'architecture (« High Level Design ») 	<ul style="list-style-type: none"> Validation des prototypes Coût de l'assistance 	<ul style="list-style-type: none"> 90% des sollicitations d'assistance pour le prototypage des projets


2.3.6 GESTION DES INCIDENTS

INC-1	Le CSP assure la gestion des incidents								
<p>Le CSP met en œuvre une gestion des incidents (au sens ITIL du terme) pour tracer, qualifier, analyser et corriger les dysfonctionnements qui entraînent une indisponibilité totale ou partielle du Service ou qui entraînent une baisse de performance rendant le Service inutilisable.</p> <p>Les incidents peuvent être détectés :</p> <ul style="list-style-type: none"> soit par le CSP. Dans ce cas il en informe le CSC ; soit par le CSC. Dans ce cas elle en informe le CSP via le support utilisateur. <p>Le CSP qualifie l'incident et son niveau de criticité et propose d'éventuelles solutions palliatives ou de contournement qui permettraient de minimiser l'impact de l'incident.</p> <p>Les niveaux de criticité sont les suivants :</p> <ul style="list-style-type: none"> Incident bloquant : l'application ou le système en production sont indisponibles pour le CSC. Il n'existe aucune solution palliative ou contournement accepté par le CSC ; Incident majeur : l'application ou le système en production sont en partie indisponibles pour le CSC ; Incident mineur : tout autre incident. <p>Les incidents de sécurité suivent cette catégorisation.</p> <p>A la demande du CSC, la criticité d'un incident peut être revue à la hausse dans le cas où il existe un ensemble d'incidents analogues ou lorsque plus de 30% des utilisateurs sont touchés.</p> <p>En cas d'incident survenant sur l'environnement de production, le CSP s'engage à rétablir la disponibilité et la performance du Service dans les délais ci-dessous :</p>									
<table border="1"> <thead> <tr> <th>Criticité de l'incident</th> <th>Délai de résolution (*)</th> </tr> </thead> <tbody> <tr> <td>Bloquant</td> <td>4 heures</td> </tr> <tr> <td>Majeur</td> <td>2 jours ouvrés</td> </tr> <tr> <td>Mineur</td> <td>5 jours ouvrés</td> </tr> </tbody> </table>		Criticité de l'incident	Délai de résolution (*)	Bloquant	4 heures	Majeur	2 jours ouvrés	Mineur	5 jours ouvrés
Criticité de l'incident	Délai de résolution (*)								
Bloquant	4 heures								
Majeur	2 jours ouvrés								
Mineur	5 jours ouvrés								
<p>(*)Le délai est calculé à partir de la déclaration de l'incident</p> <p>Le CSP fournit un reporting sur les incidents, comportant notamment les dates, heures, criticités, durées et analyses des indisponibilités.</p> <p>Le CSP doit évaluer les événements liés à la sécurité de l'information et décider s'ils doivent être classés comme incidents de sécurité. L'évaluation doit être basée sur une ou plusieurs échelles (estimation, évaluation, etc.) partagées avec le CSC.</p>									

Note : les incidents de sécurité incluent les violations de données personnelles. Le CSP doit utiliser une classification pour identifier clairement les incidents de sécurité impliquant les données du CSC, conformément aux résultats de l'évaluation des risques. Cette classification doit inclure les violations de données personnelles.


<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Analyses des incidents Solutions de contournement Résolution des incidents 	<ul style="list-style-type: none"> Délai de résolution des incidents 	<ul style="list-style-type: none"> cf. tableau ci-dessus
<ul style="list-style-type: none"> Reporting mensuel sur les incidents 	<ul style="list-style-type: none"> Délai de fourniture du reporting 	<ul style="list-style-type: none"> Reporting du mois M reçu dans les 5 premiers jours ouvrés du mois M+1


INC-2	Le CSP doit documenter et mettre en œuvre une procédure permettant de répondre rapidement et efficacement aux incidents de sécurité.	
		
<p>Le CSP doit documenter et mettre en œuvre une procédure permettant de répondre rapidement (dans le délai de résolution défini) et efficacement aux incidents de sécurité. Ces procédures doivent définir les moyens et les délais de communication des incidents de sécurité à tous les CSC concernés et le niveau de confidentialité requis pour cette communication. Le CSP doit informer ses employés et toutes les tierces parties impliquées dans la mise en œuvre du service de cette procédure. Le CSP doit documenter toute violation de données personnelles et informer son CSC.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Procédures de réponses à un incident 	<ul style="list-style-type: none"> Réception par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

INC-3	Le CSP doit gérer les incidents de sécurité et mettre en œuvre des processus pour réduire l'occurrence et l'impact des incidents.	
		
<p>Le CSP doit gérer les incidents de sécurité jusqu'à leur résolution et doit informer le CSC conformément aux procédures établies. Le CSP doit archiver les documents détaillant les incidents de sécurité.</p> <p>Le CSP doit documenter et mettre en œuvre un processus d'amélioration continue pour réduire l'occurrence et l'impact des types d'incidents de sécurité déjà traités.</p>		

Le CSP doit garantir une approche cohérente et globale pour l'identification, l'évaluation, la communication et l'escalade des incidents de sécurité.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Le CSP doit garantir une approche cohérente et globale pour l'identification, l'évaluation, la communication et l'escalade des incidents de sécurité. 	<ul style="list-style-type: none"> Communication des incidents au CSC 	<ul style="list-style-type: none"> Résolution de 100 % des incidents

INC-4	Le CSP doit documenter et mettre en œuvre une procédure pour enregistrer les informations concernant les incidents de sécurité.	
		
<p>Le CSP doit documenter et mettre en œuvre une procédure pour enregistrer les informations sur les incidents de sécurité pouvant servir de preuves.</p> <p>Le CSP surveille les événements et incidents de sécurité informatique dans le cadre du service, conformément au Plan d'Assurance de la Sécurité (PAS). Le CSP informe le CSC dans l'heure de tout événement ou incident de sécurité informatique détecté au niveau mondial sur ses infrastructures vis-à-vis de tous ses clients.</p> <p>Le CSP analyse les événements et incidents de sécurité informatique détectés, conserve et protège leurs traces, tant en termes de disponibilité que d'intégrité, afin qu'ils puissent être utilisés comme preuves en cas d'appel judiciaire.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Surveillance des événements et incidents de sécurité informatique Analyse et traces des événements et incidents de sécurité informatique 	<ul style="list-style-type: none"> Comité de sécurité 	<ul style="list-style-type: none"> Traces et analyses disponibles

<p>INC-5</p> 	<p>Le CSP doit disposer d'une ou plusieurs sondes de détection d'incidents de sécurité sur les services du système informatique</p>	
<p>Le CSP doit disposer d'une ou plusieurs sondes de détection d'incidents de sécurité sur le système informatique du service. Ces sondes doivent permettre la supervision de chacune des interconnexions du système informatique du service avec les systèmes informatiques tiers et les réseaux publics. Ces sondes doivent être des sources de collecte pour l'infrastructure d'analyse et de corrélation des événements.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Sonde de détection de sécurité 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

<p>INC-6</p>	<p>Le CSP alerte le CSC, dans les 24 heures, pour toute demande d'information ou de preuve concernant le périmètre du service</p>	
<p>Le CSP alerte le CSC, dans les 24 heures, pour toute demande d'information ou de preuve liée à un incident de sécurité, dans le cadre du service. Le CSP alerte dans l'heure si l'incident est généralisé au CSP pour l'ensemble de ses clients.</p>		
<p>L'alerte est transmise au responsable désigné au sein du CSC dans le cadre du service (à défaut, au responsable opérationnel du service ou à son supérieur).</p>		
<p>Le CSP indique dans le PAS les processus et circuits pour ces alertes.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Circuit d'alerte dans le SAP 	<ul style="list-style-type: none"> • Vérification de l'existence du circuit d'alerte dans le SAP • Nombre d'alertes 	<ul style="list-style-type: none"> • Circuit d'alerte dans le SAP • 100 % des alertes à temps

<p>INC-7</p>	<p>Le CSP alerte le CSC, sans délai, lorsqu'un événement ou incident de sécurité informatique est détecté ou lorsqu'il y a une intrusion physique sur les lieux du service.</p>	
<p>Le CSP alerte immédiatement le CSC en cas de détection d'un événement ou incident de sécurité informatique dans le cadre de son service, conformément aux procédures établies dans le SAP (PAS).</p>		

Le CSP envoie ses communications aux interlocuteurs désignés par le CSC pour la gestion des incidents de sécurité informatique (à défaut, au pilote opérationnel du service ou à son responsable), en utilisant des moyens de communication sécurisés, et conformément au processus décrit dans le SAP (PAS).

Les mêmes exigences s'appliquent en cas d'intrusion physique ou de tentative d'intrusion physique sur les lieux du service.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Alertes du CSP au CSC en cas de détection d'événements, d'incidents de sécurité informatique, d'intrusions ou de tentatives d'intrusion physique Processus de communication sur les incidents de sécurité informatique, les intrusions ou les tentatives d'intrusion physique dans le PAS 	<ul style="list-style-type: none"> Validation du processus de communication sur les incidents de sécurité informatique Nombre d'alertes 	<ul style="list-style-type: none"> 100 % des alertes sont transmises au CSC

INC-8	Le CSP assure la continuité du service en cas d'incidents, de catastrophes ou de pandémies, et doit indiquer clairement les mesures prises en cas de faillite
<p>Le CSP doit garantir la continuité du service dans les différents scénarios d'incidents, de catastrophes ou de pandémies. Le CSP doit planifier, mettre en œuvre, maintenir et tester des procédures et mesures de continuité des activités et de gestion des urgences.</p> <p>Le CSP doit documenter, mettre en œuvre et tenir à jour un plan de continuité des activités qui prend en compte la sécurité de l'information.</p> <p>Il met en place un plan de continuité des activités (PCA) qu'il teste régulièrement. À cette fin, il respectera un délai de préavis à convenir avec le CSC. Le CSC sera un contributeur au PCA. Le PCA décrit :</p> <ul style="list-style-type: none"> les mesures permanentes mises en place par le CSP pour se préparer à une reprise d'activité ; l'organisation opérationnelle pour garantir que les activités sont reprises sur une plateforme de secours dans un délai conforme aux engagements du CSP ; les modalités de test ; l'organisation pour le retour à la plateforme principale du CSP. Les résultats des tests peuvent être demandés par le CSC dans le cadre du suivi de la prestation. 	

Le CSP doit indiquer clairement les mesures prises en cas de faillite pour garantir une certaine continuité du service pendant une période de transition et permettre au CSC de récupérer tous les actifs auxquels il pourrait avoir droit.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • PCA du CSP • Plan en cas de faillite 		

2.3.7 GESTION DES ANOMALIES

AMY-1	Le CSP assure la gestion des anomalies	
<p>Le CSP met en œuvre une gestion des anomalies pour tracer, qualifier, analyser et corriger les non-conformités par rapport à une exigence spécifiée dans le présent CCTP ou à un fonctionnement attendu du Service.</p> <p>Le CSP fournit un reporting sur les anomalies, comportant notamment les références et criticités des anomalies, dates de déclaration, dates de correction et version de correction des anomalies.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Analyse des anomalies • Solutions de contournement 	<ul style="list-style-type: none"> • Délai de correction des anomalies • Nombre d'anomalies détectées par version du Service 	<ul style="list-style-type: none"> • Correction des anomalies
<ul style="list-style-type: none"> • Correctifs des anomalies 	<ul style="list-style-type: none"> • Qualité des correctifs 	
<ul style="list-style-type: none"> • Reporting mensuel sur les anomalies 	<ul style="list-style-type: none"> • Délai de fourniture du reporting 	<ul style="list-style-type: none"> • Reporting du mois M reçu dans les 5 premiers jours ouvrés du mois M+1

2.3.8 GESTION DES CRISES

CRS-1	Le CSP est partie prenante dans la gestion des crises
<p>Une situation de crise peut être déclenchée par le CSP ou par le CSC en cas de problème de fonctionnement du SERVICE, notamment dans les cas suivants :</p> <ul style="list-style-type: none"> • l'engagement de disponibilité du Service n'est pas tenu ; • des dysfonctionnements graves ou récurrents impactent le bon fonctionnement du Service ; • un comportement anormal du Service met en danger le SI du CSC ou la sécurité des données ; <p>... et que ces problèmes ne peuvent plus être gérés par les acteurs et les procédures habituels.</p>	

Des crises peuvent également être déclenchées via une procédure d'escalade en cas de différend persistant entre le CSP et le CSC, notamment lorsqu'une situation pourrait mettre en péril le planning ou la qualité des prestations, par exemples dans les cas suivants :

- Non-respect récurrent des délais de livraison des livrables ;
- Absence de réponse aux demandes de support ;
- Désaccord sur des décisions à prendre ;
- Dysfonctionnement lié à une mauvaise qualité de service ;
- Dysfonctionnement au niveau de la communication interne ou externe.

Le CSP doit s'impliquer dans le suivi des crises même si leur origine n'est pas de sa responsabilité et il agit en coordination avec l'ensemble des acteurs concernés du CSC pour sortir au plus vite des crises.

Dès le démarrage de la crise, le CSC et le CSP organisent une réunion pour établir un diagnostic de la situation, évaluer les risques et mettre en place des moyens et une organisation permettant de gérer la crise. LE CSC et le CSP conviennent d'un plan d'actions pour résoudre les problèmes et revenir au plus vite vers une situation normale. Une fois la crise terminée, le CSC et le CSP font un retour d'expérience.

Les modalités d'intervention du CSP feront l'objet d'un paragraphe spécifique du PAQ ainsi que dans le PAS ou autre document équivalent. A minima, l'intervention du CSP se fera en mode audio.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Analyse de crise 	<ul style="list-style-type: none"> • Contribution à la gestion de crise 	<ul style="list-style-type: none"> • Contact disponible chez le CSP
<ul style="list-style-type: none"> • Retour d'information et plan d'action 	<ul style="list-style-type: none"> • Réception des retours d'information 	<ul style="list-style-type: none"> • Retour d'information reçu moins de 10 jours après le début de crise


2.3.9 GESTION DES RISQUES

RSK-1	Le CSP fournit des procédures de gestion des risques.
<p>Il doit être assuré que les risques liés à la sécurité de l'information sont correctement identifiés, évalués et traités, et que le risque résiduel est formellement accepté par la direction du CSP.</p> <p>L'analyse des risques doit être examinée par le CSP annuellement et chaque fois qu'il y a un changement majeur susceptible d'avoir un impact sur le service.</p> <p>Le CSP doit effectuer son évaluation des risques à l'aide d'une méthode documentée garantissant la reproductibilité et la comparabilité de l'approche.</p> <p>Le CSP doit prendre en compte dans l'évaluation des risques :</p> <ul style="list-style-type: none"> • La gestion des informations provenant des CSC ayant des besoins de sécurité différents. • Les risques impactant les droits et libertés des personnes concernées en cas d'accès non autorisé, de modification non désirée et de disparition de données personnelles. 	

- Les risques de défaillance des mécanismes de partitionnement des ressources d'infrastructure technique (mémoire, calcul, stockage, réseau) partagées entre les CSC.
- Les risques liés à la suppression incomplète ou non sécurisée des données stockées dans la mémoire ou les espaces de stockage partagés entre les CSC, notamment lors de la réaffectation de la mémoire et des espaces de stockage.
- Les risques associés à l'exposition des interfaces administratives sur un réseau public.
- Les risques associés à l'accumulation de responsabilités ou de tâches.
- Les risques associés à une pénurie de ressources dans un ou plusieurs des datacenters du CSP. Il doit garantir qu'en cas de saturation, il existe une procédure claire pour garantir la qualité (et plus précisément l'élasticité) des services.


Lorsqu'il existe des exigences spécifiques légales, réglementaires ou sectorielles relatives aux types d'informations que le CSC peut confier au CSP, ce dernier doit en tenir compte dans son évaluation des risques en veillant à se conformer à toutes les exigences de ce document de référence d'une part, et à ne pas abaisser le niveau de sécurité établi par la conformité aux exigences de ce document de référence d'autre part.


<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Analyse des risques • Procédures d'évaluation des risques 	<ul style="list-style-type: none"> • Réception des documents par le CSC • Réunion annuelle pour examiner les risques 	<ul style="list-style-type: none"> • Accord de la direction du CSC sur les risques • Validation des procédures

RSK-2	Le CSP documente une évaluation des risques pour un projet ayant un impact sur les SERVICES.	
		
<p>Le CSP doit documenter une évaluation des risques avant tout projet pouvant avoir un impact sur le SERVICE, quelle que soit la nature du projet. Si un projet affecte ou est susceptible d'affecter le niveau de sécurité du service, le CSP doit en informer le CSC et les informer par écrit des impacts potentiels, des mesures mises en place pour réduire ces impacts et des risques résiduels les affectant.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Évaluation des risques 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Accord de la direction du CSC sur les risques
<ul style="list-style-type: none"> • <u>Niveau de Confiance (BONUS)</u> : Le CSP assiste le CSC dans la réalisation de leur étude d'impact sur la protection des données 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Si le CSP est conscient d'un risque élevé de traitement en raison d'une étude d'impact sur la protection des données réalisée à l'avance par le CSC, le CSP doit prendre des


		mesures appropriées aux risques.
--	--	----------------------------------

2.3.10 GESTION DES ACTIFS


ASM-1 	Le CSP fournit un inventaire dynamique des actifs.	
<p>Il est essentiel d'identifier les actifs de l'organisation et de garantir un niveau de protection approprié tout au long de leur cycle de vie. Cet inventaire doit être maintenu à jour.</p> <p>Le CSP doit documenter et mettre en œuvre une procédure de retour des actifs pour garantir que chaque personne impliquée dans la prestation du service restitue tous les actifs en sa possession à la fin de son emploi ou de son contrat.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Inventaire des actifs • Processus de retour 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

ASM-2 	Le CSP tient à jour une cartographie des SERVICES	
<p>Le CSP doit établir et maintenir à jour une cartographie du système informatique du service, liée à l'inventaire des actifs, comprenant au moins les éléments suivants :</p> <ul style="list-style-type: none"> • La liste des ressources matérielles ou virtualisées ; • Les noms et fonctions des applications, supportant le service ; • Le diagramme d'architecture réseau au niveau 3 du modèle OSI sur lequel les points névralgiques sont identifiés : <ul style="list-style-type: none"> ○ Les points d'interconnexion, notamment avec les réseaux tiers et publics, ○ Les réseaux, sous-réseaux, en particulier les réseaux d'administration, ○ Les équipements assurant des fonctions de sécurité (filtrage, authentification, chiffrement, etc.), ○ Les serveurs hébergeant des données ou exécutant des fonctions sensibles, ○ La matrice des flux réseau autorisés, précisant : <ul style="list-style-type: none"> ○ Leur description technique (services, protocoles et ports), ○ La justification par ligne métier ou infrastructure, ○ Le cas échéant, lorsque des services, protocoles ou ports jugés non sécurisés sont utilisés, les mesures compensatoires mises en place, dans une optique de défense en profondeur. <p>Le CSP doit revoir la cartographie au moins une fois par an.</p>		


Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Cartographie des services 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

ASM-3 	Propos complémentaire : Il est conseillé au CSP de documenter et de mettre en œuvre une procédure pour le marquage et la gestion de toutes les informations impliquées dans la prestation du service
<p>Il est conseillé au CSP de documenter et de mettre en œuvre une procédure pour le marquage et la gestion de toutes les informations impliquées dans la prestation du service, conformément à ses besoins en matière de sécurité.</p>	

2.3.11 SÉCURITÉ DES LOCAUX ET DU PERSONNEL

FCPS-1 	Le CSP garantit la sécurité physique de ses installations et sites
<p>Si les services sont fournis sur un ou plusieurs sites du CSP, ce dernier met en œuvre des mesures pour protéger le périmètre physique du service, conformément à la politique de contrôle d'accès de référence (celle du CSP ou celle du CSC, selon le type de service).</p> <p>Le CSP doit documenter et mettre en œuvre :</p> <ul style="list-style-type: none"> • Les moyens pour minimiser les risques inhérents aux catastrophes physiques (incendie, dégâts des eaux, etc.) et naturelles (risques climatiques, inondations, tremblements de terre, etc.) ; • Des mesures pour limiter le risque de déclenchement ou de propagation d'incendies, ainsi que les risques de dégâts des eaux ; • Des mesures pour prévenir et limiter les conséquences d'une panne de courant et permettre la reprise du service conformément aux exigences de disponibilité de service définies dans l'accord de service ; • Les moyens de maintenir des conditions de température et d'humidité appropriées pour l'équipement. De plus, il doit mettre en œuvre des mesures pour prévenir les défaillances de climatisation et en limiter les conséquences ; • Des contrôles et des tests réguliers de l'équipement de détection et de protection physique ; • Des moyens doivent être mis en œuvre pour empêcher l'accès physique non autorisé et se protéger contre le vol, les dommages, les pertes et les pannes opérationnelles. <p>Le CSP effectue des contrôles physiques et environnementaux pour protéger le service proportionnellement au niveau de risque, et informe le CSC des résultats obtenus.</p> <p>Ces contrôles doivent être effectués à une fréquence pertinente (par exemple, une fois par an).</p>	

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Résultats des vérifications effectuées par le CSP 	<ul style="list-style-type: none"> Rapport des résultats au CSC 	<ul style="list-style-type: none"> Résultats validés par le CSC


FCPS-2 	Le CSP doit documenter et mettre en œuvre des périmètres de sécurité.
<p>Le CSP doit documenter et mettre en œuvre des périmètres de sécurité, y compris le marquage des zones et les différents moyens de limiter et de contrôler l'accès. Le CSP doit distinguer entre les zones publiques, les zones privées et les zones sensibles :</p> <p>Les zones publiques sont accessibles à tous à l'intérieur des limites de la propriété du CSP. Le CSP ne doit pas héberger de ressources dédiées au service ou permettant l'accès à des composants du service dans les zones publiques. Les zones de livraison et de chargement ainsi que d'autres points où des personnes non autorisées peuvent entrer dans les locaux sans accompagnement sont considérées comme des zones publiques. Le CSP doit isoler les points d'accès de ces zones vers les zones privées et sensibles, afin d'empêcher tout accès non autorisé, ou mettre en œuvre des mesures compensatoires pour assurer le même niveau de sécurité.</p> <p>Les zones privées peuvent héberger les plates-formes de développement et les installations du service, les stations d'administration, d'exploitation et de supervision ainsi que les locaux à partir desquels le CSP opère. Le CSP doit :</p> <ul style="list-style-type: none"> Protéger les zones privées contre l'accès non autorisé. Pour ce faire, il doit mettre en œuvre un contrôle d'accès physique basé sur au moins un facteur personnel : la connaissance d'un secret, la possession d'un objet ou la biométrie. Définir et documenter des mesures exceptionnelles d'accès physique pour les situations d'urgence. Afficher un avertissement à l'entrée des zones privées concernant les restrictions et conditions d'accès à ces zones. Définir et documenter les créneaux horaires et les conditions d'accès aux zones privées en fonction des profils des parties concernées. Documenter et mettre en œuvre les moyens pour garantir que les visiteurs sont systématiquement accompagnés par le CSP lors de l'accès et du séjour dans la zone privée. Le CSP doit tenir un registre de l'identité des visiteurs conformément aux lois et réglementations en vigueur. Documenter et mettre en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones privées. <p>Les zones sensibles sont réservées à l'hébergement du système informatique de production du service, à l'exclusion des stations d'administration, d'exploitation et de supervision. Le CSP doit :</p>	

- Protéger les zones sensibles contre l'accès non autorisé. Pour ce faire, il doit mettre en œuvre un contrôle d'accès physique basé sur au moins deux facteurs personnels : la connaissance d'un secret, la possession d'un objet ou la biométrie.
- Définir et documenter des mesures exceptionnelles d'accès physique pour les situations d'urgence.
- Afficher un avertissement à l'entrée des zones sensibles concernant les restrictions et conditions d'accès à ces zones.
- Définir et documenter les créneaux horaires et les conditions d'accès aux zones sensibles en fonction des profils des parties concernées.
- Documenter et mettre en œuvre les moyens pour garantir que les visiteurs sont systématiquement accompagnés par le CSP lors de l'accès et du séjour dans la zone sensible. Le CSP doit tenir un registre de l'identité des visiteurs conformément aux lois et réglementations en vigueur.
- Documenter et mettre en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones sensibles.
- Mettre en œuvre la journalisation des accès physiques aux zones sensibles. Il doit examiner ces journaux au moins une fois par mois.
- Mettre en place des moyens pour garantir qu'aucun accès direct n'existe entre une zone publique et une zone sensible.


Le CSP doit intégrer les éléments de sécurité physique dans la politique de sécurité et l'évaluation des risques conformément au niveau de sécurité requis par la catégorie de la zone. Le CSP doit documenter et mettre en œuvre des procédures de travail dans les zones privées et sensibles. Il doit communiquer ces procédures aux parties concernées.


Dans le cadre du contrôle d'accès physique, le CSP doit se conformer aux normes publiées par les autorités compétentes (ANSSI, BSI, etc.).


<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Description des scopes de sécurité et des procédures • Résultats des vérifications effectuées par le CSP 	<ul style="list-style-type: none"> • Réception des reportings par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC


FCPS-3 	Le CSP doit documenter et mettre en œuvre des mesures pour séparer physiquement les environnements de production des services des autres environnements.
<p>Le CSP doit documenter et mettre en œuvre des mesures pour séparer physiquement les environnements de production du service des autres environnements, y compris les environnements de développement.</p>	


<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Distribution des environnements 	<ul style="list-style-type: none"> Réception des documents 	<ul style="list-style-type: none"> Validation des documents


FCPS-4	Le CSP doit documenter et mettre en œuvre des mesures pour protéger les câbles électriques et de télécommunication.	
		
<p>Le CSP doit documenter et mettre en œuvre des mesures pour protéger les câbles électriques et de télécommunication contre les dommages physiques et les interceptions éventuelles. Le CSP doit produire un plan de câblage et le tenir à jour.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Plan de sécurité des brassages 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

FCPS-5	Le CSP doit garantir la sécurité dans les zones privées et sensibles pendant les périodes d'installation et de maintenance.	
		
<p>Le CSP doit documenter et mettre en œuvre des mesures pour garantir que les conditions d'installation, de maintenance et de service de l'équipement informatique du service hébergé dans les zones privées et sensibles sont compatibles avec les exigences de confidentialité et de disponibilité du service telles que définies dans l'accord de service. Le CSP doit souscrire des contrats de maintenance pour garantir que les mises à jour de sécurité sont disponibles pour les logiciels installés sur l'équipement informatique du service. Le CSP doit veiller à ce que les supports ne puissent être retournés à un tiers que si les données du CSC qui y sont stockées sont chiffrées conformément au chapitre "Cryptographie" ou ont été préalablement détruites en utilisant un mécanisme d'effacement sécurisé par réécriture de motifs aléatoires. Le CSP doit documenter et mettre en œuvre des mesures pour garantir que les conditions d'installation, de maintenance et de service de l'équipement technique auxiliaire (alimentation électrique, climatisation, incendie, etc.) sont compatibles avec les exigences de disponibilité du service telles que définies dans l'accord de service.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Les procédures d'installation et de maintenance du CSP 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation of the documents by the CSC

FCPS-6 	Le CSP doit documenter et mettre en œuvre une procédure pour le transfert hors site des données, équipements et logiciels du CSC.	
<p>Le CSP doit documenter et mettre en œuvre une procédure pour le transfert hors site des données, équipements et logiciels du CSC. Cette procédure doit exiger une autorisation écrite de la direction du CSC. Dans tous les cas, le CSP doit mettre en œuvre les moyens pour garantir que le niveau de protection en termes de confidentialité et d'intégrité des actifs pendant le transport est équivalent à celui sur site.</p> <p>Le CSP doit documenter et mettre en œuvre une procédure pour protéger les équipements en attente d'utilisation.</p> <p>Le CSP doit documenter et mettre en œuvre une procédure pour la gestion des supports amovibles qui est adaptée aux besoins de sécurité des services de données avec lesquels ils peuvent être confiés par les clients. Lorsque des supports amovibles sont utilisés sur l'infrastructure technique ou pour des tâches administratives, ces supports doivent être dédiés à un seul usage.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Procédure de transfert hors site • Procédure de gestion des supports amovibles 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

FCPS-7 	Le CSP vérifie les informations concernant son personnel	
<p>Le CSP doit documenter et mettre en œuvre une procédure pour la vérification des informations concernant son personnel, conformément aux lois et réglementations applicables. Ces vérifications s'appliquent à tous ceux impliqués dans la fourniture du service et doivent être proportionnées à la sensibilité des informations confiées au CSP par le client et aux risques identifiés.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Procédure de vérification des informations du personnel 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

<p>FCPS-8</p> 	<p>Le CSP doit sensibiliser ses parties prenantes aux problèmes de sécurité liés aux CSC.</p>	
<p>Le CSP doit régulièrement sensibiliser ses parties prenantes aux problèmes de sécurité informatique. Cette sensibilisation doit accompagner les thèmes abordés dans le livret d'accueil. De plus, le CSP doit disposer d'une charte éthique intégrée aux règles et règlements internes, stipulant notamment que :</p>		
<ul style="list-style-type: none"> • Les services sont fournis avec loyauté, discrétion, impartialité et dans le respect de la confidentialité des informations traitées. • Le personnel n'utilise que des méthodes, des outils et des techniques validés par le CSP. • Le personnel s'engage à ne pas divulguer à un tiers toute information, même anonymisée et décontextualisée, obtenue ou générée dans le cadre du service, sauf autorisation formelle écrite du CSC. • Le personnel s'engage à signaler au CSP tout contenu manifestement illégal découvert pendant le service. • Le personnel s'engage à se conformer aux lois et réglementations nationales en vigueur et aux bonnes pratiques relatives à leurs activités. 		
<p>Le CSP doit faire signer la charte éthique à toutes les parties impliquées dans la prestation de service. De plus, sur demande du CSC, le CSP doit mettre à leur disposition les règles internes et la charte éthique.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Règles internes et charte éthique • Programme et fréquence des sessions de sensibilisation à la sécurité 	<ul style="list-style-type: none"> • Contrôler par le CSC 	<ul style="list-style-type: none"> • 100% des employés signent la charte

<p>FCPS-9</p> 	<p>Le CSP doit disposer d'un plan de formation en matière de sécurité et de processus disciplinaires en cas de violations des politiques de sécurité.</p>	
<p>Le CSP doit sensibiliser tous ceux impliqués dans la prestation du service aux risques liés à la sécurité de l'information et à la protection des données. Il doit les informer de toute mise à jour des politiques et des procédures pertinentes à leurs missions. Le CSP doit documenter et mettre en œuvre un plan de formation en sécurité de l'information adapté au service et aux tâches du personnel. L'officier de sécurité des systèmes d'information du CSP doit valider formellement le plan de formation en sécurité de l'information.</p>		

Le CSP doit s'assurer que ses employés comprennent leurs responsabilités, sont conscients de leur responsabilité en matière de sécurité de l'information, et que les actifs de l'organisation sont protégés en cas de changement de responsabilité ou de cessation d'emploi.


Le CSP doit documenter et mettre en œuvre une sensibilisation de ses employés aux risques liés aux codes malveillants et aux bonnes pratiques pour réduire l'impact d'une infection.

Le CSP doit documenter et mettre en œuvre un processus disciplinaire applicable à toutes les personnes impliquées dans la prestation du service ayant enfreint la politique de sécurité. Le CSP doit, sur demande du CSC, mettre à leur disposition les sanctions encourues pour violation de la politique de sécurité.


Le CSP, via l'officier de sécurité de l'information, doit régulièrement s'assurer que toutes les procédures de sécurité dont il est responsable sont correctement exécutées pour garantir la conformité aux politiques et normes de sécurité.

Le CSP doit définir et attribuer des rôles et responsabilités pour la résiliation, la conclusion ou la modification de tout contrat avec une personne impliquée dans la prestation du service.


<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Engagement sur les politiques de sécurité 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

FCPS-10	Le CSP doit documenter et mettre en œuvre une procédure exigeant que ses employés et les tiers impliqués dans la mise en œuvre du service leur signalent tout incident de sécurité connu ou suspecté et toute violation	
		
<p>Le CSP doit documenter et mettre en œuvre une procédure exigeant que ses employés et les tiers impliqués dans la mise en œuvre du service leur signalent tout incident de sécurité connu ou suspecté ainsi que toute violation. De plus, le CSP doit documenter et mettre en œuvre une procédure permettant à tous les CSC de signaler tout incident de sécurité ou toute vulnérabilité connus ou suspectés. Le CSP doit informer sans délai le CSC des incidents de sécurité et des recommandations associées pour limiter leur impact. Il doit permettre au CSC de choisir le niveau de gravité des incidents dont ils souhaitent être informés. Le CSP doit également signaler les incidents de sécurité aux autorités compétentes conformément aux exigences légales et réglementaires applicables.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Processus de reporting d'incident 	<ul style="list-style-type: none"> Réception par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

2.3.12 GESTION DES VULNÉRABILITÉS

VLM-1 	Le CSP corrige les vulnérabilités dont il a connaissance sur ses solutions.	
<p>Le CSP s'engage à respecter un délai pour corriger les vulnérabilités découvertes sur ses livraisons et portées à sa connaissance, en fonction de la gravité de la vulnérabilité. Les délais doivent être conformes aux bonnes pratiques en matière de sécurité.</p> <p>Lorsque l'existence d'une vulnérabilité est rendue publique avant la disponibilité du correctif (0-day), le CSP doit informer immédiatement le CSC. Le CSP fournit au CSC une solution dès que possible. Si le correctif n'est pas disponible dans les deux jours ouvrables, il doit proposer une solution de contournement au CSC pour éviter le risque.</p> <p>Le CSP doit documenter et mettre en œuvre un processus de surveillance pour gérer les vulnérabilités techniques des logiciels et des systèmes utilisés dans le système informatique du service. Le CSP doit évaluer son exposition à ces vulnérabilités en les intégrant dans l'analyse des risques et appliquer des mesures de gestion des risques appropriées.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Politique de Livraison des correctifs • Procédure de Surveillance des Vulnérabilités Techniques 	<ul style="list-style-type: none"> • Réception des livrables 	<ul style="list-style-type: none"> • 100% des vulnérabilités corrigées dans les délais • 100% des vulnérabilités 0-day notifiées au CSC sans délai • 100% des vulnérabilités 0-day contournées dans les délais
<ul style="list-style-type: none"> • Engagement dans le PAS 	<ul style="list-style-type: none"> • Vérification de l'engagement dans le PAS 	


2.3.13 OPÉRABILITÉ


OPY-1 	Le CSP doit documenter les procédures opérationnelles.	
<p>Le CSP doit documenter les procédures opérationnelles, les maintenir à jour et les rendre disponibles au personnel concerné. Le CSP doit documenter et mettre en œuvre une procédure de gestion des changements apportés aux systèmes de traitement de l'information et aux installations. Le CSP doit documenter et mettre en œuvre une procédure permettant de communiquer le plus</p>		


rapidement possible à l'ensemble de ses parties contractantes les opérations effectuées par le prestataire de services et susceptibles d'avoir un impact sur la sécurité ou la disponibilité du service :


- La date et l'heure prévues du début et de la fin des opérations,
- La nature des opérations,
- Les impacts sur la sécurité ou la disponibilité du service,
- La personne de contact au sein du CSP.


<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Procédures opérationnelles • Procédures de gestion du changement 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

OPY-2	Le CSP doit informer le CSC de toute modification future des éléments logiciels.	
		
<p>Dans le cadre d'un service PaaS, le CSP doit informer le CSC dès que possible de toute modification future des éléments logiciels dont il est responsable si une compatibilité totale ne peut être assurée. Dans le cas d'un service SaaS, le CSP doit informer le client dès que possible de toute modification future des éléments du service pouvant entraîner une perte de fonctionnalité pour le CSC.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Reporting du changement 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC


OPY-3	Le CSP doit documenter et mettre en œuvre une procédure de contrôle de l'installation de logiciels sur l'équipement informatique du service.	
		
<p>Le CSP doit documenter et mettre en œuvre une procédure de contrôle de l'installation de logiciels sur l'équipement informatique du service. Le CSP doit également documenter et mettre en œuvre une procédure de gestion de la configuration des environnements logiciels mis à disposition du CSC, notamment pour les maintenir protégés.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Procédure de contrôle d'installation des logiciels 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

<p>OPY-4</p> 	<p>Le CSP doit documenter et mettre en œuvre une procédure de suivi des modifications apportées au système informatique du service.</p>	
<p>Le CSP doit documenter et mettre en œuvre une procédure de suivi des modifications apportées au système informatique du service. Le CSP doit également documenter et mettre en œuvre une procédure de validation des modifications apportées au système informatique du service dans un environnement de pré-production avant leur mise en production. Le CSP doit conserver un historique des versions des logiciels et des systèmes (développements internes ou externes, produits commerciaux et métiers) mis en œuvre pour permettre de reconstituer un environnement complet, si nécessaire, dans un environnement de test, tel qu'il était mis en œuvre à une date donnée. La période de rétention de cet historique doit être conforme à la période de rétention des sauvegardes. Le CSP doit s'assurer que les modifications et les actions de configuration des systèmes informatiques garantissent la sécurité du service cloud fourni.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Procédure de gestion du changement 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

<p>OPY-5</p> 	<p>Le CSP doit documenter et mettre en œuvre une procédure pour tester toutes les applications avant leur mise en production.</p>	
<p>Le CSP doit documenter et mettre en œuvre une procédure pour tester toutes les applications avant leur mise en production afin de garantir qu'il n'y a pas d'effets indésirables sur l'activité ou la sécurité du service.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Procédure de Test 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

<p>OPY-6</p> 	<p>Le CSP garantit l'intégrité des données en préproduction</p>	
<p>Le CSP doit documenter et mettre en œuvre une procédure pour garantir l'intégrité des données de test utilisées en préproduction. Si le CSP souhaite utiliser les données de production du client pour effectuer des tests, il doit d'abord obtenir l'approbation du CSC et anonymiser les données. Le CSP doit veiller à la confidentialité des données lors de leur anonymisation.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Procédure de garantie de l'intégrité des 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

données de pré-production		
---------------------------	--	--

OPY-7 	Le CSP fournit des solutions compatibles avec le monitoring de la sécurité.	
<p>Le CSP doit documenter et mettre 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 informatique du service, en temps réel ou ultérieurement pour les événements datant jusqu'à six mois. Le CSP doit accuser réception des alarmes déclenchées par l'infrastructure d'analyse et de corrélation des événements au moins une fois par jour.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Reporting des logs d'infrastructure 	<ul style="list-style-type: none"> Réception par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

OPY-8 	Le CSP doit mettre en place un environnement de développement sécurisé.	
<p>Le CSP doit mettre en place un environnement de développement sécurisé pour gérer l'ensemble du cycle de développement du système informatique du service. Le CSP doit prendre en compte les environnements de développement dans l'évaluation des risques et assurer leur protection conformément à ce document de référence.</p> <p>Le CSP doit documenter et mettre en œuvre une procédure de supervision et de contrôle de l'activité de développement de logiciels et de systèmes externalisée. Cette procédure doit garantir que l'activité de développement externalisée est conforme à la politique de développement sécurisé du CSP et atteint un niveau de sécurité équivalent à celui d'un développement interne.</p> <p>Le CSP doit tester les nouveaux systèmes informatiques ou les mises à jour pour leur conformité et leur fonctionnalité de sécurité pendant le développement. Il doit documenter et mettre en œuvre une procédure de test qui identifie :</p> <ul style="list-style-type: none"> Les tâches à effectuer, Les données d'entrée, Les résultats attendus. 		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Environnement de développement 	<ul style="list-style-type: none"> Réception et test par le CSC 	<ul style="list-style-type: none"> Validation par le CSC Disponibilité 24/7

<ul style="list-style-type: none"> • Procédure de supervision des logiciels externalisés • Procédure de test 		
--	--	--

2.4 GOUVERNANCE ET GESTION OPÉRATIONNELLE

2.4.1 GOUVERNANCE

GOV-1	Le CSP nomme un seul responsable de la livraison	
<p>Le CSP nomme un seul gestionnaire de service, ayant le pouvoir d'organiser opérationnellement la livraison du service, dont les principales responsabilités sont les suivantes :</p> <ul style="list-style-type: none"> • gérer la relation opérationnelle avec le CSC ; • assurer le suivi du service, des délais et des coûts ; • veiller à ce que les engagements soient respectés et que les niveaux de service définis soient atteints ; • garantir l'amélioration continue du service fourni au CSC ; • gérer la résolution rapide et efficace des dysfonctionnements pouvant survenir sur le service ; • consolider les informations nécessaires pour le reporting et les diffuser au CSC. <p>Il devrait contacter en priorité une personne de contact dédiée au sein du CSC.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
		<ul style="list-style-type: none"> • Désignation de la seule partie responsable

2.4.2 GESTION DE LA QUALITÉ

GOV-2	Le CSP garantit la qualité et la sécurité du service au travers de son plan d'assurance qualité.	
<p>Le CSP établit des processus, une organisation et des ressources pour garantir la qualité et la sécurité du service et de ses dispositions. Ils élaborent un Plan d'Assurance Qualité & Sécurité (PAQS), comprenant, au minimum tous les processus et activités du service :</p> <ul style="list-style-type: none"> • L'organisation, les rôles et les responsabilités des acteurs du CSP. • Les méthodes de communication entre le CSC et le CSP. • Les règles d'interaction entre le CSC et le CSP (réunions, mode de suivi (indicateurs), reporting au responsable du service, suivi des progrès, suivi des actions, suivi budgétaire, prise de décision et suivi, suivi des risques, gestion des incidents). • La fréquence des réunions planifiées. • Organisation du reporting et ses délais de livraison. • Processus de gestion de crise. 		

- Gestion de la documentation (organisation de la documentation, identification et classification des documents, etc.).
- Gestion des incidents, gestion des problèmes, gestion des anomalies, gestion des changements et gestion du déploiement en production.
- Gestion des écarts par rapport aux périmètres définis dans le CCTP. Contexte opérationnel.
- Articulation du service en phases, activités et tâches à réaliser.
- Environnement méthodologique (méthodes et outils de gestion, conception, implémentation, test du service).
- Modalités et dispositifs pour atteindre les jalons du service.
- Description du Plan de Réversibilité et du Plan de Mise en Œuvre de la Réversibilité.
- Plan d'Assurance Sécurité (PAS) tel que défini au paragraphe 3.2.

Le CSP s'engage à apporter toutes les mises à jour nécessaires pendant le service, le cas échéant, pour garantir que le PAQS reflète le service réalisé. Toute modification du PAQS est soumise au Comité de Pilotage. Le CSC dispose de deux semaines pour valider le PAQS, puis le CSP dispose d'une semaine pour prendre en compte les commentaires du CSC.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • PAQS 	<ul style="list-style-type: none"> • Délai initial de livraison du PAQS 	<ul style="list-style-type: none"> • Livraison au plus tard 30 jours ouvrables après la date de début du contrat

GOV-3	Le CSP s'engage à mettre en œuvre des politiques efficaces de Responsabilité Sociale des Entreprises (RSE)	
L'organisation doit faire preuve d'un engagement envers des pratiques durables, une conduite éthique et un impact social en participant activement à des initiatives bénéfiques pour l'environnement, les employés, les communautés locales et d'autres parties prenantes.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Politiques RSE 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Description complètes des politiques RSE

2.4.3 REPORTING ET INDICATEURS

GOV-4	Le CSP doit produire un rapport mensuel présentant les indicateurs de résultats de surveillance attendus par le CSC
Le CSP doit produire un rapport mensuel présentant les indicateurs de résultats de surveillance attendus par le CSC ainsi qu'une analyse de ces indicateurs et de leur évolution dans le temps. Il s'engage à fournir ce rapport dans un délai de 5 jours ouvrables au plus tard après la fin du mois M concerné.	

Le CSP doit décrire précisément dans le PAQS la méthode de détermination des indicateurs (données mesurées ou calculées, date/heure des mesures, algorithme de calcul, outil à partir duquel les données sont extraites, etc.). Ces indicateurs peuvent évoluer d'un commun accord entre le CSC et le CSP.

Le CSC décide d'accepter ou non les indicateurs présentés. Le Comité de pilotage analyse les écarts par rapport aux engagements de service demandés par le CSC et le CSC détermine les éventuelles pénalités à appliquer. Si les seuils d'acceptabilité sont dépassés, le CSP s'engage à fournir un plan d'action qui sera soumis au CSC pour validation.

Le CSP doit tenir un registre à jour des opérations de traitement.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Reporting 	<ul style="list-style-type: none"> Timeline du reporting 	<ul style="list-style-type: none"> Le rapport pour le mois M est reçu dans les 5 premiers jours ouvrables du mois M+1
<ul style="list-style-type: none"> Plan d'action 	<ul style="list-style-type: none"> Date limite de livraison du plan d'action 	<ul style="list-style-type: none"> Plan d'action reçu dans les 10 jours ouvrables suivant la réunion du Comité de pilotage

2.4.4 COMITOLOGIE

GOV-5	Le CSP contribue au Comité de pilotage mensuel
	<p>Ce comité mensuel, qui peut être bimensuel par décision des deux parties, fournit les informations nécessaires et suffisantes au CSC et au CSP pour gérer le service. Il se concentre sur les points forts du mois précédent et présente les éléments pouvant avoir un impact stratégique ou contractuel sur le fonctionnement du service.</p> <p>Ce comité fait l'objet d'une réunion préparatoire qui se tient dans les cinq jours ouvrables précédents.</p> <ul style="list-style-type: none"> Objectifs principaux : <ul style="list-style-type: none"> Validation de la facturation mensuelle ; Examen des changements apportés au Service et des tarifs associés ; Examen des indicateurs contractuels pour le suivi de la performance ; Analyse des dysfonctionnements ; Gestion des divergences de service et des pénalités ; Examen des difficultés rencontrées, ainsi que des alertes ; Examen des différents points contractuels, y compris la sous-traitance ; Révision de la sécurité ; Présentation des développements émanant du CSC ; Présentation de la feuille de route pour l'évolution du service CSP ; Présentation des domaines d'amélioration dans l'utilisation des services afin de réduire la facture. Lieu :

- Ces comités se tiennent dans les locaux du CSC en région parisienne et en personne. Par décision des deux parties, certains comités peuvent se tenir par audio/webconférence.
- Compte-rendu :
 - Le compte-rendu est rédigé par le CSP et envoyé au CSC pour validation dans un délai de trois jours ouvrables.

Ce dernier dispose de cinq jours ouvrables pour valider ce compte-rendu.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> ● Comptes-rendus des comités de pilotage 	<ul style="list-style-type: none"> ● Délais de soumission des comptes-rendus ● Qualité des comptes-rendus 	<ul style="list-style-type: none"> ● Compte rendu reçu dans les 5 jours ouvrables suivant le Comité de Pilotage ● < 2 réexpéditions

GOV-6	Le CSP participe au Comité de Suivi Contractuel	
<p>En plus des comités de pilotage mensuels, le CSC se réserve le droit de mettre en place un Comité de Suivi Contractuel à tout moment, s'il le juge nécessaire. Ce comité facultatif peut être nécessaire en cas d'incident bloquant, d'incident majeur de sécurité ou de tout autre élément ou événement majeur nécessitant une discussion entre les deux parties avant la prochaine réunion du Comité de Pilotage.</p> <ul style="list-style-type: none"> ● Lieu: <ul style="list-style-type: none"> ○ Ces comités se tiennent dans les locaux du CSC situés dans la région parisienne et en personne. Par décision des deux parties, certains comités peuvent se tenir par audio/conférence web. ● Compte-rendu : <ul style="list-style-type: none"> ○ Le compte-rendu est rédigé par le CSP et envoyé au CSC pour validation dans un délai de trois jours ouvrables. Ce dernier dispose de trois jours ouvrables pour valider ce rapport. 		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> ● Comptes-rendus des comités de pilotage contractuel 	<ul style="list-style-type: none"> ● Délais de soumission des comptes-rendus ● Qualité des comptes-rendus 	<ul style="list-style-type: none"> ● Compte rendu reçu dans les 5 jours ouvrables suivant le Comité de Pilotage ● < 2 réexpéditions

GOV-7	The CSP participe au Comité de Pilotage semestrielle	
<p>Ce comité semestriel permet au CSC et au CSP de discuter des évolutions majeures du service et de son utilisation par le CSC, afin d'anticiper ensemble l'évolution générale du service.</p> <ul style="list-style-type: none"> • Objectifs principaux : <ul style="list-style-type: none"> ○ Présentation de la feuille de route pour l'évolution du Service par le CSP ; ○ Présentation des changements dans le CSC susceptibles d'impact sur son utilisation du Service. • Lieu : <ul style="list-style-type: none"> ○ Ces comités se tiennent en personne dans les locaux du CSC. Par décision des deux parties, certains comités peuvent être tenus par audioconférence/web. • Compte rendu : <ul style="list-style-type: none"> ○ Le Compte rendu est rédigé par le CSP et envoyé au CSC pour validation dans un délai de cinq jours ouvrables. Ce dernier dispose de cinq jours ouvrables pour valider ce rapport. 		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Comptes-rendus des comités de pilotage 	<ul style="list-style-type: none"> • Délais de soumission des comptes-rendus • Qualité des comptes-rendus 	<ul style="list-style-type: none"> • Compte rendu reçu dans les 5 jours ouvrables suivant le Comité de Pilotage • < 2 réexpéditions

3 SÉCURITÉ

3.1 EXIGENCES DE SÉCURITÉ

3.1.1 POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION (PSSI)

SECU-1	Le CSP s'engage à respecter la PSSI du CSC pendant toute la durée du contrat	
<p>Le CSP doit respecter la Politique de Sécurité des Systèmes d'Information (PSSI) du CSC. Cette dernière peut être consultée par le CSP, sur demande, dans les locaux du CSC.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Engagement du CSP (dans le PAS) 	<ul style="list-style-type: none"> Réception du PAS par ce CSC Audits par le CSC 	<ul style="list-style-type: none"> PAS validé par le CSC Le CSP peut être conforme avec 100% de la PSSI du CSC

SECU-2	Le CSP s'engage à définir sa PSSI et à l'appliquer	
<p>Le CSP s'engage à disposer d'une Politique de Sécurité des Systèmes d'Information (PSSI) conforme à l'état de l'art et à l'appliquer.</p> <p>Le CSP doit mettre à jour sa PSSI a minima une fois par an et doit informer le CSC lorsque les évolutions de la PSSI sont susceptibles d'impacter le CSC.</p> <p>La PSSI doit être consultable par le CSC à tout moment sur demande. A défaut, le CSP s'engage à fournir une description de sa PSSI, ainsi que des éléments qui justifient que celle-ci soit bien conforme à l'état de l'art.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> PSSI du CSC 	<ul style="list-style-type: none"> Notifications du CSP au CSC en cas de modification de l'PSSI Consultation de l'PSSI du CSP par le CSC 	<ul style="list-style-type: none"> Contrôle de l'PSSI du CSP par le CSC Le CSC est en accord avec l'PSSI du CSP

3.1.2 PLAN D'ASSURANCE DE SÉCURITÉ (PAS)

SAP-1	Le CSP rédige et maintient un Plan d'Assurance de la Sécurité (PAS)
<p>Conformément aux bonnes pratiques de l'ANSSI, le CSP s'engage à fournir un PAS pour préciser l'ensemble de ses engagements, et décrire l'organisation mise en place pour répondre aux exigences du CSC.</p>	

Ce document décrira notamment les différents processus mis en place dans le cadre de la prestation, les acteurs, les documents et données échangés ainsi que leur fréquence.

Le PAS est soumis aux mêmes règles de livraison et de validation que le Plan d'Assurance Qualité (PAQ) et peut y être intégré sous forme d'un document unique (PAQS).

Le PAS reprendra tous les engagements présents dans cette annexe et contiendra à minima l'ensemble des conditions d'exécution des prestations suivantes :

1. Organisation de la sécurité des SI en interne au sein du CSP, en mode nominal ainsi qu'en mode dégradé ;
2. Identification des rôles et responsabilités en matière de sécurité des SI ;
3. Modalités de protection des ressources requises dans le cadre de ce contrat, y compris la politique de protection des systèmes portables ;
4. Gestion des ressources humaines et maintenance des compétences en matière de sécurité des SI ;
5. Identification et gestion des actifs ;
6. Gestion de l'accès physique au site, aux locaux et aux ressources ;
7. Gestion de l'accès à l'information ;
8. Gestion des supports d'information ;
9. Gestion des supports et supports mis au rebut (documents papier ou informatiques) ;
10. Identification et gestion des risques liés à la sécurité des SI et des vulnérabilités techniques ;
11. Gestion des incidents de sécurité des SI et processus de notification en cas de fuite de données personnelles ;
12. Contrôles internes et audits de sécurité des SI ;
13. Tableaux de bord et indicateurs liés à la sécurité des SI ;
14. Gestion de la continuité d'activité des plates-formes de télé-exploitation/télé-administration ;
15. Gestion de crise en cas d'incident de sécurité des SI ;
16. Conformité aux exigences légales et réglementaires (notamment conservation des dossiers, désignation d'un DPO, gestion du traitement de l'exercice des droits, etc.) ;

Ce document doit identifier les engagements du CSP pour se conformer à la législation et aux réglementations pertinentes. Le CSC reste responsable de la conformité aux contraintes légales et réglementaires applicables aux données qu'il confie au CSP.

Le CSP s'engage à fournir une version initiale (v0) du PAS avec sa réponse. Cette v0 peut être l'un des éléments contractuels et servira de base de sécurité minimale pour la durée du service.


Le CSP est libre d'adopter le formalisme qu'il juge approprié. Le CSP s'engage à fournir la version finalisée (V1) du PAS au plus tard un mois après le début du service. Le PAS est soumis à validation par le CSC. Ses modalités d'évolution doivent être spécifiées.

Enfin, le CSP initie les mises à jour (au moins annuelles) du PAS qu'il fait évoluer en fonction des besoins. Le CSC peut également contribuer à son évolution, notamment en ce qui concerne les processus de gestion des incidents, la gestion de crise, etc.

Le CSP informe le CSC de chaque modification apportée au PAS.


Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • VO du PAS • Version finalisée (V1) du PAS 	<ul style="list-style-type: none"> • Réception des livrables par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC 30 jours après le début du contrat


3.1.3 CONTACT DE SECURITÉ DU SYSTÈME D'INFORMATION (CSSI)


ISSC-1	Le CSP désigne une personne de contact en matière de sécurité des systèmes d'information dans le cadre des services cloud	
		
<p>Le CSP s'engage à désigner une personne de contact en matière de sécurité chargée de la sécurité du SERVICE, que ce soit dans la phase de construction ou dans un régime récurrent, c'est-à-dire capable de :</p> <ul style="list-style-type: none"> • Informer le CSC en cas d'incident ou de demande liée au respect des exigences décrites dans ce document, • Prendre des mesures pour limiter les effets immédiats d'un incident ou pour y remédier, • Prendre des décisions si des arbitrages sont nécessaires dans la gestion d'un incident, • Répondre à l'ensemble du périmètre du SERVICE (y compris les sous-traitants ou cocontractants). <p>Cette personne de contact (ou ses suppléants en cas d'absence) doit être joignable pendant les heures de travail par le CSC.</p> <p>Le SAP précisera le nom et les coordonnées de cette personne de contact ainsi que les modalités de contact de ses suppléants en cas d'indisponibilité.</p> <p>Il est essentiel de planifier, de mettre en œuvre, de maintenir et d'améliorer continuellement le cadre de sécurité de l'information au sein de l'organisation. Cette organisation comprend la nomination d'un responsable de la sécurité des systèmes d'information et d'un responsable de la sécurité physique (si nécessaire).</p> <p>De plus, le CSP s'engage à disposer d'un contact opérationnel disponible 24 heures sur 24 et 7 jours sur 7 que le CSC peut appeler pour signaler tout incident de sécurité et prendre des mesures si nécessaire. Les détails et modalités de ce contact doivent être précisés dans le SAP.</p> <p>Le CSP informe le CSC lorsqu'il nomme un nouveau contact en matière de sécurité.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Désignation d'une personne de contact en matière de sécurité des systèmes d'information au sein du CSP • PAS incluant les coordonnées et les modalités de contact 	<ul style="list-style-type: none"> • Réunion en face-à-face ou en vidéoconférence avec l'interlocuteur en sécurité des SI • Validation de l'engagement du CSP dans le SAP 	<ul style="list-style-type: none"> • Contact(s) identifié(s) joignable(s) en cas d'incident

de la personne désignée		
-------------------------	--	--


3.1.4 MESURES DE CONTRÔLE ET D'AUDIT

AUD-1 	Propos introductif : Le CSP établit des relations appropriées avec les autorités compétentes et les groupes de spécialistes.
<p>Le CSP est encouragé à établir des relations appropriées avec les autorités compétentes (approuvées par les autorités européennes ou nationales) pour la sécurité des informations et des données personnelles, et le cas échéant, avec les autorités sectorielles, en fonction de la nature des informations confiées par le CSC au CSP.</p> <p>Le CSP est encouragé à maintenir des contacts appropriés avec des groupes spécialisés ou des sources reconnues, notamment afin de prendre en compte les nouvelles menaces et les mesures de sécurité appropriées pour les contrer.</p>	

AUD-2 	Le CSP doit coopérer avec le CSC dans le suivi et les audits réalisés par le CSC.	
<p>Le CSC se réserve le droit d'effectuer des vérifications et des audits sur le périmètre du service qui le concerne. Le CSP coopère avec le CSC dans le cadre des contrôles et des audits. En particulier, le CSP met à disposition des contrôleurs et des auditeurs mandatés par le CSC, sans frais supplémentaires, toutes les ressources nécessaires pour mener à bien les contrôles et les audits (avant ou pendant leur réalisation). Le CSC doit :</p> <ul style="list-style-type: none"> • Effectuer des contrôles de l'exécution du contrat ; • Réaliser des audits des services ; • Effectuer des audits de sécurité (sur les applications et les infrastructures informatiques dédiées au CSC) ; • Procéder à des extractions de données (sauvegardées) selon les procédures du CSP ; • Effectuer des vérifications de conformité avec le SAP. Le CSP doit documenter et mettre en œuvre un programme d'audit triennal définissant la portée et la fréquence des audits conformément à la gestion des changements, aux politiques et aux résultats de l'évaluation des risques. 		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Fourniture par le CSP des éléments permettant les audits et les contrôles par le CSC 	<ul style="list-style-type: none"> • Audits et contrôles par le CSC 	<ul style="list-style-type: none"> • Coopération atteinte


<p>AUD-3</p> 	<p>Le CSP met en place des contrôles internes et des audits</p>	
<p>Le CSP met en place des contrôles internes et des audits sur le périmètre du service afin de garantir le respect des éléments suivants :</p> <ul style="list-style-type: none"> • Règles et procédures de sécurité IS du CSC ; • Engagements contractuels. <p>Le CSP fournit au CSC un calendrier provisoire des audits et des contrôles, ainsi que les résultats obtenus.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Programme provisoire des audits et des contrôles internes du CSP • Résultats des audits et des contrôles internes 	<ul style="list-style-type: none"> • Réception des résultats des audits et des contrôles internes du CSP par le CSC 	<ul style="list-style-type: none"> • Programme provisoire accepté par le CSC • 100% du programme provisoire respecté par le CSP • 100% des résultats reçus par le CSC

<p>AUD-4</p> 	<p>Le CSP doit indiquer la liste des entreprises (et leur nationalité) autorisées à réaliser des audits.</p>	
<p>Le CSP doit indiquer la liste des entreprises (et leur nationalité) autorisées à réaliser des audits. Niveau de confiance requis : Les audits sont effectués par des entreprises approuvées par les autorités européennes (ANSSI, BSI, etc.).</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> • Liste des entreprises d'audit 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • <u>Niveau de confiance requis</u> : Les audits sont effectués par des entreprises approuvées par les autorités européennes (ANSSI, BSI, etc.).


<p>AUD-5</p> 	<p>Le CSP doit signaler les demandes d'enquête de l'État au CSC</p>	
<p>Le CSP doit signaler les demandes d'enquête de l'État au CSC.</p>		

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Engagement du CSP dans le SAP 	<ul style="list-style-type: none"> Vérification de l'engagement dans le PAS par le CSC 	<ul style="list-style-type: none"> Engagement dans le PAS


3.1.5 SÉCURITÉ DES INFORMATIONS

ISEC-1	Le CSP doit identifier les différents besoins en matière de sécurité pour les informations relatives au service.	
		
<p>Le CSP doit identifier les différents besoins en matière de sécurité pour les informations relatives au service. Lorsque le CSC peut confier au CSP des données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques, le CSP doit identifier les exigences de sécurité spécifiques associées à ces contraintes.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Exigences spécifiques en matière de sécurité pour les contraintes légales, réglementaires ou sectorielles 	<ul style="list-style-type: none"> Réception par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

ISEC-2	Le CSP doit spécifier tous les processus qu'il prend en charge pour maintenir l'intégrité des données, la continuité du service et la prévention de la perte de données spécifiques à l'importation de données	
<p>Le CSP doit spécifier tous les processus qu'il prend en charge pour maintenir l'intégrité des données, assurer la continuité du service et prévenir la perte de données spécifiques à l'importation de données (par exemple, sauvegarde et vérification des données avant et après le transfert, temps d'arrêt et transmission sécurisée, fonctionnalité de retour en arrière et toute fonctionnalité de test).</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Procédure d'importation de données 	<ul style="list-style-type: none"> Réception par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

ISEC-3 	Le CSP doit documenter et mettre en œuvre une procédure pour répondre rapidement et efficacement aux incidents de sécurité.	
<p>Le CSP doit documenter et mettre en œuvre une procédure pour répondre rapidement et efficacement aux incidents de sécurité. Ces procédures doivent définir les moyens et les délais de communication des incidents de sécurité à tous les CSC concernés ainsi que le niveau de confidentialité requis pour une telle communication. Le CSP doit informer ses employés et toutes les tierces parties impliquées dans la mise en œuvre du service de cette procédure. Le CSP doit documenter toute violation de données personnelles et informer son CSC.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Procédure de réponse à un incident 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

ISEC-4	Les conditions générales d'utilisation régissant les droits des parties à utiliser le service et les données sont formalisées.	
<p>Les conditions générales d'utilisation régissant les droits des parties à utiliser le service et les données sont formalisées. Le CSP doit inclure des dispositions régissant les droits d'auteur ou autres droits de propriété intellectuelle.</p> <p>Le CSP doit explicitement indiquer sur son site Web les juridictions régissant l'infrastructure conformément à l'article 28 du Data Act.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Conditions générales d'utilisation (CGU) • Politiques de droit d'auteur et de propriété intellectuelle du CSP 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Conformité avec les politiques du CSC

ISEC-5 	Le CSP s'engage à effacer de manière irréversible les informations du CSC lorsque cela est nécessaire.	
<p>Le CSP doit mettre en place un plan de destruction des informations dans des conditions garantissant leur confidentialité après accord et conformément aux directives du CSC et dans le respect de l'environnement.</p> <p>En cas de mise hors service d'une ressource contenant des informations ou des données appartenant au CSC (exemples : serveur, machine virtuelle, poste de travail, stockage, etc.), le CSP met en œuvre un plan visant à supprimer les données présentes sur cette ressource dans des</p>		

conditions garantissant la suppression définitive et irréversible de toutes les données et sauvegardes relatives à la ressource.

À la résiliation ou à l'expiration du contrat, quelle qu'en soit la cause, le CSP remet immédiatement, sauf instruction contraire du CSC, à ce dernier tous les originaux et copies des registres, archives, livres, documents relatifs au contrat, ainsi que toute autre information, imprimé, matériel fourni par le CSC, acquis ou préparé par le CSP, directement ou indirectement lié au CSC et au contrat.


Le format de récupération des données doit être basé sur une norme définie entre le CSP et le CSC.


À la demande du CSC, le CSP certifie par écrit que lesdits fichiers, archives, livres, documents, informations, imprimés, matériaux n'ont pas été conservés ou copiés par le CSP ou ses sous-traitants.

Le CSP ne doit supprimer les données du CSC de ses systèmes qu'après avoir reçu une approbation écrite explicite du CSC.


En cas de faillite du CSC, cette approbation doit être donnée par la personne responsable de la liquidation du CSC.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Plan de destruction des données Engagement du CSP dans le PAS 	<ul style="list-style-type: none"> Demandes de consentement du CSP avant la suppression des données du CSC Vérification de la présence de l'engagement du CSP dans le SAP Réception du plan de destruction des données Destruction HP 	<ul style="list-style-type: none"> Présence de l'engagement du CSP dans le PAS Aucune donnée du CSC n'a été supprimée sans consentement préalable du CSC Le plan de destruction des données est validé par le CSC


ISEC-6	Le CSP doit documenter et mettre en œuvre des moyens pour effacer de manière sécurisée tout support de données mis à disposition du CSC.	
	<p>Le CSP doit documenter et mettre en œuvre des moyens pour effacer de manière sécurisée tout support de données mis à disposition du CSC en réécrivant des motifs aléatoires. Si l'espace de stockage est chiffré avec les mécanismes spécifiés dans le chapitre "cryptographie", l'effacement peut être réalisé en effaçant de manière sécurisée la clé de chiffrement.</p>	
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Procédure d'effacement des données sur les médias 	<ul style="list-style-type: none"> Réception par le CSC 	<ul style="list-style-type: none"> Validation par le CSC


ISEC-7 	Le CSP doit permettre l'accès au service cloud via d'autres services cloud afin d'obtenir les données stockées et de les supprimer	
<p>Le CSP doit permettre l'accès au service cloud via d'autres services cloud ou systèmes informatiques des CSC, afin d'obtenir les données stockées à la fin de la relation contractuelle et de les supprimer de manière sécurisée.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Procédure d'accès externe aux données 	<ul style="list-style-type: none"> • Réception des documents et tests par le CSP 	<ul style="list-style-type: none"> • Validation par le CSP


3.1.6 CHIFFREMENT DES DONNÉES ET CERTIFICATS

CRPT-1 	Le CSP doit être en mesure de chiffrer les données sensibles.	
<p>Le CSC doit être en mesure de chiffrer ses données sensibles ("au repos" (stockées) et "en transit" (transférées)). Le CSC est le seul détenteur de la clé de chiffrement de ses données et la période de révocation de la clé doit être inférieure à 7 jours. Le CSP fournit au CSC les outils nécessaires pour chiffrer ses données et propose également un outil de validation des secrets. Le CSC doit être en mesure de déchiffrer les données chiffrées par le CSP. Pour ce faire, il doit disposer de la clé de chiffrement de ses données. Les données doivent également être utilisables après déchiffrement. Le CSC doit pouvoir utiliser des clés de chiffrement tierces. Le CSC est le seul détenteur de la clé de chiffrement de ses données et la période de révocation de la clé doit être inférieure à 7 jours.</p>		
<p>Le CSP fournit au CSC les outils nécessaires pour chiffrer ses données et propose également un outil de validation des secrets.</p>		
<p>Le CSC doit être en mesure de déchiffrer les données chiffrées par le CSP. Pour ce faire, il doit disposer de la clé de chiffrement de ses données. Les données doivent également être utilisables après déchiffrement.</p>		
<p>Le CSC doit pouvoir utiliser des clés de chiffrement tierces.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Service ou outil de chiffrement 	<ul style="list-style-type: none"> • Utilisation et test de l'outil de chiffrement 	<ul style="list-style-type: none"> • Disponibilité 7j/7, 24h/24


CRPT-2		Le CSP fournit un outil de gestion des certificats.	
<p>Le CSP fournit au CSC un outil de gestion des certificats. Le CSC souhaite avoir la possibilité d'utiliser une solution tierce interopérable avec le cloud du CSP pour répondre à ce besoin (importation de certificats ou gestion de bout en bout). Le CSP fournit alors une liste de solutions interopérables avec son cloud.</p> <p>Le CSP doit être en mesure de mettre en œuvre des certificats délivrés au CSC par une "autorité de confiance".</p>			
Livrable(s) :		Contrôle des résultats :	Objective(s):
<ul style="list-style-type: none"> Service ou outil de gestion des certificats 		<ul style="list-style-type: none"> Utilisation du service ou de l'outil de gestion des certificats 	<ul style="list-style-type: none"> Disponibilité 24/7

CRPT-3		Le CSP doit définir et mettre en œuvre un mécanisme de chiffrement qui empêche la récupération des données du CSC en cas de réaffectation d'une ressource ou de récupération du support physique	
			
<p>Le CSP doit définir et mettre en œuvre un mécanisme de chiffrement qui empêche la récupération des données du CSC en cas de réaffectation d'une ressource ou de récupération du support physique. Dans le cas d'un service IaaS, cet objectif peut être atteint, par exemple :</p> <ul style="list-style-type: none"> Par le chiffrement du disque ou du système de fichiers, où le protocole d'accès en mode fichier garantit que seuls des blocs vides peuvent être alloués (par exemple, le stockage de type NAS dans lequel un bloc physique n'est effectivement alloué qu'au moment de l'écriture) ; Par le chiffrement basé sur le volume dans le cas d'un accès par bloc (par exemple, NAS ou stockage local), avec au moins une clé par CSC ; Dans le cas d'un service PaaS ou SaaS, cela peut être réalisé en utilisant le chiffrement au niveau de l'application dans le cadre du CSP, avec au moins une clé par CSC. <p>Le CSP doit mettre en œuvre le chiffrement des données sur les supports amovibles et les supports de sauvegarde qui doivent être emportés en dehors du périmètre de sécurité physique du système informatique du service, en fonction des besoins de sécurité des données.</p>			
Livrable(s) :		Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Description des mécanismes de chiffrement 		<ul style="list-style-type: none"> Réception des documents et tests par le CSP 	<ul style="list-style-type: none"> Validation par le CSP

CRPT-4 	Le CSP doit fournir un catalogue de méthodes de chiffrement des données permettant au CSC de se conformer aux règles de ses autorités compétentes.	
<p>Le CSP doit proposer un catalogue de méthodes de chiffrement des données permettant au CSC de se conformer aux règles de ses autorités compétentes. De plus, le CSP doit utiliser des clés de chiffrement conformes aux recommandations des autorités compétentes pertinentes (ANSSI, BSI, etc.) lors de :</p> <ul style="list-style-type: none"> • La mise en place d'un mécanisme de chiffrement des flux réseau ; • Le stockage de l'empreinte des mots de passe utilisateur et des comptes techniques. Les empreintes doivent être générées avec une fonction de hachage associée à l'utilisation d'un scellement numérique ; • La mise en place d'un mécanisme de signature électronique ; • L'utilisation de clés de chiffrement. 		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Catalogue de méthodes de chiffrement des données 	<ul style="list-style-type: none"> • Réception par le CSP 	<ul style="list-style-type: none"> • Validation par le CSP

CRPT-5 	Le CSP doit protéger l'accès aux clés de chiffrement et autres secrets utilisés pour le chiffrement des données	
<p>Le CSP doit protéger l'accès aux clés de chiffrement et autres secrets utilisés pour chiffrer les données selon des moyens appropriés : conteneur de sécurité (logiciel ou matériel) ou support séparé. Le CSP doit également protéger l'accès aux clés de chiffrement et autres secrets utilisés pour les tâches administratives à l'aide d'un conteneur de sécurité approprié, logiciel ou matériel.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Description des mesures de sécurités 	<ul style="list-style-type: none"> • Réception par le CSP 	<ul style="list-style-type: none"> • Validation par le CSP

3.1.7 TRAÇABILITÉ

TRAC-1 	Le CSP met en œuvre l'enregistrement des accès et du traitement des données du CSC (y compris les sauvegardes).	
<p>Le CSP doit documenter et mettre en œuvre une politique de journalisation comprenant au minimum les éléments suivants :</p>		

- La liste des sources de collecte,
- La liste des événements à journaliser par source,
- Le but de la journalisation des événements,
- La fréquence de collecte et la base temporelle utilisée,
- Le temps de rétention local et centralisé,
- Les mesures de protection des journaux (y compris le chiffrement et la duplication),
- L'emplacement des journaux,

Le CSP doit générer et collecter les événements suivants :

- Les activités des utilisateurs liées à la sécurité de l'information,
- Les changements de droits d'accès dans sa zone de responsabilité,
- Les événements des mécanismes anti-programme malveillant,
- Les modifications de données sensibles,
- Les exceptions,
- Les échecs,
- Tout autre événement lié à la sécurité de l'information.

Le CSP doit conserver les événements de journalisation pendant un minimum de six mois, sous réserve du respect des exigences légales et réglementaires. Le CSP doit fournir, sur demande d'une partie contractante, tous les événements concernant ladite partie.

Le protocole utilisé et le format des journaux seront convenus entre le CSC et le CSP.

Les journaux doivent être envoyés en temps réel au CSC ou avec un retard annoncé et contrôlable : si l'application doit être surveillée par le Centre opérationnel de sécurité (SOC) du CSC, les journaux devront être envoyés au CSC.

Le CSP doit protéger l'équipement de journalisation et les événements journaux contre les attaques sur leur disponibilité, intégrité ou confidentialité. Le CSP doit gérer le dimensionnement de l'espace de stockage de tout équipement hébergeant une ou plusieurs sources de collecte afin de permettre le stockage local des événements journaux anticipés par la politique de journalisation des événements. Cette gestion de dimensionnement doit prendre en compte les changements du système informatique.


Le CSP doit transférer les événements journaux collectés, en veillant à ce que leur confidentialité et leur intégrité soient protégées, vers un ou plusieurs serveurs centraux dédiés, et doit les stocker sur une machine physique séparée de celle qui les a générés.

Le CSP doit mettre en œuvre une sauvegarde des événements collectés basée sur une politique appropriée.


Le CSP doit effectuer les processus de journalisation et de collecte d'événements à l'aide de comptes avec des privilèges nécessaires et suffisants et doit limiter l'accès aux événements journaux conformément à la politique de contrôle d'accès.

Le CSP doit préciser quels sont, le cas échéant, les données d'audit de sécurité qui peuvent être importées (par exemple, les journaux des interactions des utilisateurs avec le service cloud qui peuvent être nécessaires pour l'analyse de sécurité et pour surveiller les demandes).

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Journaux d'activité des données du CSC, par application • Données d'audit de sécurité pouvant être importées 	<ul style="list-style-type: none"> • Contrôlé par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7 • Validation de la qualité des journaux par le CSC

TRAC-2	Le CSP doit documenter et mettre en œuvre une synchronisation des horloges.	
	<p>Le CSP doit documenter et mettre en œuvre une synchronisation des horloges de tout l'équipement vers une ou plusieurs sources de temps internes cohérentes entre elles. Ces sources peuvent elles-mêmes être synchronisées avec plusieurs sources externes fiables, sauf pour les réseaux isolés. Le CSP doit mettre en œuvre le marquage temporel de chaque événement enregistré</p>	
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Procédure de synchronisation des horloges 	<ul style="list-style-type: none"> • Contrôlé par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC


3.1.8 PARTITIONNEMENT

PART-1	Le CSP doit documenter et mettre en œuvre, pour le système informatique du service, des mesures de partitionnement pour séparer les flux réseau.	
	<p>Le CSP doit documenter et mettre en œuvre, pour le système informatique du service, des mesures de partitionnement (logique, physique ou par chiffrement) pour séparer les flux réseau en fonction de :</p> <ul style="list-style-type: none"> • La sensibilité des informations envoyées, • La nature des flux (production, administration, supervision, etc.), • Le domaine auquel appartiennent les flux (des CSC - distingués par CSC ou tous les CSC, du CSP, de tiers, etc.), • Le domaine technique (traitement, stockage, etc.). <p>Le CSP doit partitionner tous les flux de données internes au système informatique du service par rapport à tout autre système informatique, soit physiquement, soit par chiffrement. Lorsque ce partitionnement est réalisé par chiffrement, il doit être effectué conformément aux exigences du chapitre "cryptographie". Si le réseau d'administration de l'infrastructure technique n'est pas physiquement partitionné, les flux d'administration doivent passer par un tunnel chiffré, conformément aux exigences du chapitre "cryptographie".</p>	

Le CSP doit mettre en place et configurer un pare-feu applicatif pour protéger les interfaces d'administration de ses CSCs qui sont exposées sur un réseau public.

Le CSP doit mettre en œuvre un mécanisme de filtrage sur toutes les interfaces d'administration et de supervision de l'infrastructure technique du service, n'autorisant que les connexions légitimes identifiées dans la matrice des flux autorisés.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Description des Silos Logiques des Données CSC 	<ul style="list-style-type: none"> Contrôlé par le CSC 	<ul style="list-style-type: none"> Données des CSC isolées logiquement et vérifiées par le CSC

PART-2	Le CSP met en œuvre des mesures de partitionnement appropriées	
		
<p>Le CSP doit mettre en œuvre des mesures de partitionnement appropriées :</p> <ul style="list-style-type: none"> entre ses CSC. entre le système informatique du service et ses autres systèmes informatiques (bureautique, informatique interne au CSC, gestion technique du bâtiment, contrôle d'accès physique, etc.). au minimum entre l'infrastructure technique d'une part et les équipements nécessaires à l'administration des services et des ressources qu'elle héberge d'autre part. 		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Schéma d'architecture technique 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

PART-3	Le CSP doit assurer la privatisation des services managés	
<p>Lorsque le CSP utilise un service IaaS comme base d'un autre type de service (PaaS ou SaaS), les ressources allouées à l'usage du CSP ne doivent en aucun cas être accessibles via l'interface publique mise à disposition des autres CSC du service IaaS. Lorsque le CSP utilise un service PaaS comme base d'un autre type de service (typiquement SaaS), les ressources allouées à l'usage du CSP ne doivent en aucun cas être accessibles via l'interface publique mise à disposition des autres CSC du service PaaS.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Schéma d'architecture technique 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

3.1.9 SÉCURITÉ DES COMMUNICATIONS

CSEC-1	Le CSP doit chiffrer ses communications électroniques avec le CSC si des données sensibles sont présentes	
<p>Dans le cadre du service, le CSP et le CSC communiquent par des moyens informatiques tels que la messagerie électronique, la messagerie instantanée, les espaces collaboratifs, etc. Certaines informations provenant du CSC sont sensibles. Il est nécessaire de garantir une utilisation appropriée et efficace du chiffrement pour assurer la confidentialité, l'authenticité ou l'intégrité des informations. Pour cette raison, le CSP et le CSC doivent conjointement identifier celles qui nécessitent que les communications électroniques (par tous moyens) entre les deux parties soient systématiquement chiffrées. Ce chiffrement s'applique indépendamment de l'emplacement du CSP. Pour le chiffrement des messages électroniques et des pièces jointes, le CSP et le CSC conviendront des moyens à utiliser (ceux du CSC et/ou ceux du CSP).</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Procédure de communication de données sensibles 	<ul style="list-style-type: none"> • Réception des documents et tests par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

CSEC-2	Le CSP fournit des composants de partage de données conformes	
<p>Les composants utilisés pour le partage de données doivent :</p> <ul style="list-style-type: none"> • fournir un degré de confiance et de sécurité suffisamment élevé en ce qui concerne l'intégrité, la confidentialité et la disponibilité des informations échangées. • vérifier l'authenticité et l'intégrité de tous les composants du système avant l'exécution. • enregistrer chaque décision de contrôle d'accès, chaque accès aux données, chaque modification de sa configuration et chaque instance où un service reçoit moins de ressources que demandé en tant qu'entrée de journal protégée par intégrité dans son domaine. 		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Description des composants de partage de données 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

CSEC-3	Le CSP permet l'utilisation d'identités numériques fédérées (BONUS).	
<p>Lors du transfert de données, le consommateur et le fournisseur de données doivent chacun identifier leur organisation au moyen d'identités numériques unifiées.</p>		

Le consommateur et le fournisseur de données doivent identifier les composants utilisés pour le partage et le traitement des données via des identités numériques fédérées.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Description des composants de partage de données 	<ul style="list-style-type: none"> Réception des documents par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

3.1.10 PATCH DE SÉCURITÉ


PTC-1	Le CSP doit appliquer les correctifs de sécurité pour les vulnérabilités signalées par le CERT-FR et le SOC du CSC	
<p>Cela s'applique aux ressources du CSC pour lesquelles le CSP est responsable ainsi qu'aux ressources du CSP utilisées dans le cadre du service.</p> <p>En cas d'alerte grave (attaque virale, faille critique) annoncée par des organismes tels que le CERTA/CERT-FR (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), la correction doit être appliquée dans un délai qui respecte la qualification du CSC sur les ressources concernées.</p> <p>Lorsqu'aucun correctif n'est disponible, le CSP doit suivre les recommandations du fournisseur de la solution ou du CERTA/CERT-FR dans le cadre d'une solution temporaire. Si le contournement nécessite la désactivation d'une fonctionnalité essentielle au système, le CSP s'engage à proposer des mesures de contournement. Le CSP fournit un rapport sur son intervention (plan de réduction des vulnérabilités) au CSC et lors du comité de sécurité. Les modalités d'application des mesures correctives seront convenues entre le CSC et le CSP</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Alertes fournies par le CERT-FR Plan de résorption des vulnérabilités critiques 	<ul style="list-style-type: none"> Communication des alertes au CSC Comité de sécurité 	<ul style="list-style-type: none"> 100 % des alertes rapportées au CSC 100 % des correctifs de sécurité appliqués dans le délai convenu entre le CSC et le CSP

3.1.11 ACCÈS ET IDENTITÉS

AID-1	Propos introductif : Responsabilités du CSP et du CSC
	<p>Il est essentiel de limiter l'accès aux installations de traitement de l'information ainsi qu'à l'information elle-même.</p>


Sauf indication contraire explicite, ce chapitre traite de la gestion des accès et de l'identification des utilisateurs :


- Pour lesquels le CSP est responsable (ses employés et éventuellement des tiers impliqués dans la prestation de service),
- Pour lesquels le CSC est responsable, mais pour lesquels le prestataire de service met en œuvre les moyens de contrôle d'accès (en particulier en fournissant au CSC une interface de gestion des comptes et des droits d'accès).

AID-2 	Le CSP fournit sa politique de contrôle d'accès	
<p>Le CSP doit documenter et mettre en œuvre une politique de contrôle d'accès basée sur le résultat de son évaluation des risques et sur le partage des responsabilités.</p> <p>Le CSP doit revoir la politique de contrôle d'accès annuellement et chaque fois qu'il y a un changement majeur susceptible d'avoir un impact sur le service. Les procédures suivantes doivent figurer dans la politique de contrôle d'accès :</p> <ul style="list-style-type: none"> • Procédure d'inscription et de désinscription des utilisateurs basée sur une interface de gestion des comptes et des droits d'accès. Cette procédure doit indiquer quelles données doivent être supprimées lorsqu'un utilisateur quitte le service. • Désinscription d'un utilisateur entraînant la suppression de tout accès aux ressources informatiques du service et la suppression des données de l'utilisateur conformément à la procédure d'inscription et de désinscription. • Processus d'attribution de comptes nommés par le CSP lors de l'inscription des utilisateurs sous sa responsabilité. • L'octroi, la modification et le retrait des droits d'accès aux ressources informatiques du service 		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Politique de contrôle des accès 	<ul style="list-style-type: none"> • Réception des documents par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

AID-3	Le CSP fournit une solution de gestion des identités et des accès	
<p>Le CSP fournit au CSC une solution d'authentification des utilisateurs sur les portails d'administration du CSP et pour les applications de chaque projet (en utilisant par exemple un courtier d'identité). Le CSC souhaite avoir la possibilité d'utiliser son outil de gestion centralisée des identités.</p>		

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outil de gestion des accès et identités 	<ul style="list-style-type: none"> Tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

AID-4	Le CSP fournit un outil de gestion des droits d'accès des utilisateurs pour les services	
		
<p>Le CSP doit fournir au CSC un outil lui permettant de gérer les rôles et les droits d'accès des utilisateurs pour les différents services. Cet outil doit permettre de :</p> <p>Différencier les rôles des utilisateurs du service, par exemple en fonction de leur rôle fonctionnel.</p> <p>Maintenir un inventaire à jour des utilisateurs dont il est responsable, qui disposent de droits d'administration pour les ressources informatiques du service.</p> <p>Accorder, pour une ressource donnée mettant en œuvre le service, une liste de tous les utilisateurs y ayant accès, qu'ils relèvent de la responsabilité du CSP ou du CSC, ainsi que les droits d'accès qui leur ont été attribués.</p> <p>Fournir, pour un utilisateur donné, qu'il relève de la responsabilité du CSP ou du CSC, une liste de tous ses droits d'accès aux différents éléments du système informatique du service.</p> <p>Faciliter l'examen des droits d'accès des utilisateurs pour lesquels le CSP et le CSC sont responsables.</p> <p>Le CSP doit inclure dans la procédure de gestion des droits d'accès les actions de révocation ou de suspension des droits de tout utilisateur.</p> <p>Le CSP doit revoir annuellement les droits d'accès des utilisateurs dont il est responsable et trimestriellement la liste des utilisateurs dont il est responsable et qui peuvent utiliser les comptes techniques.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outil de gestion des accès et des rôles des utilisateurs Procédure de gestion des droits d'accès 	<ul style="list-style-type: none"> Réception des documents et des tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7 Validation par le CSC

AID-5	Le CSP fournit un outil de contrôle d'accès aux services	
		
<p>Le CSP fournit au CSC une solution de contrôle d'accès aux services de la plateforme cloud et aux ressources. Cet outil doit également offrir des solutions d'authentification à la plateforme MFA. Au</p>		

minimum, l'outil doit être capable de fournir un mécanisme de restriction d'accès basé sur l'adresse IP et/ou une authentification forte (multifacteur, certificats, etc.).

Le CSP doit formaliser et mettre en œuvre des procédures de gestion de l'authentification des utilisateurs. Celles-ci doivent inclure :

- La gestion des moyens d'authentification (émission et réinitialisation des mots de passe, mise à jour des listes de révocation des certificats (CRL) et importation des certificats racine lors de l'utilisation de certificats, etc.).
- La mise en œuvre des moyens permettant une authentification multifacteur pour répondre aux différents cas d'utilisation du document de référence.
- Des systèmes qui génèrent des mots de passe ou vérifient leur robustesse, lorsque l'authentification par mot de passe est utilisée. Les règles définissant la robustesse nécessaire du mot de passe doivent être personnalisables par le CSC.

Tous les mécanismes d'authentification doivent permettre le blocage d'un compte après un nombre limité de tentatives infructueuses.


<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outil de contrôle d'accès aux services • Outil de gestion de l'authentification des utilisateurs 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC


AID-6	Les services du CSP doivent être équipés d'une gestion des identités compatible avec les normes standards d'échange d'authentification.	
<p>Dans le cas où les outils de gestion des identités du CSC seraient utilisés pour authentifier et accéder aux applications du CSP, ce dernier doit proposer une gestion des identités compatible avec les normes de protocoles d'échange d'authentification : OIDC, SAML, OAuth, OpenID, LDAPS.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Gestion des identités compatible avec SAML 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC de la compatibilité

AID-7	Le CSP fournit un accès sécurisé aux services SaaS	
<p>Dans le cadre d'un service SaaS, le CSP doit fournir au CSC des moyens d'authentification multifacteurs pour l'accès des utilisateurs finaux.</p>		

Lorsque des comptes techniques non nominatifs sont nécessaires sur le service SaaS, le CSP doit fournir au CSC les moyens d'exiger des utilisateurs de se connecter en utilisant leur compte nominatif avant de pouvoir accéder à ces comptes techniques.


Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • MFA pour des services SaaS • Connexion personnelle avant l'utilisation d'un moyen de connexion générique 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7


AID-8	Le CSP fournit un environnement sécurisé pour les comptes et interfaces d'administration	
		
<p>Pour garantir un environnement sécurisé pour les comptes et interfaces d'administration, le CSP doit :</p> <ul style="list-style-type: none"> • Gérer les comptes d'administration relevant de sa responsabilité à l'aide d'outils et de répertoires distincts de ceux utilisés pour la gestion des comptes d'utilisateur relevant de la responsabilité du CSC. • Utiliser une interface d'administration différente pour le CSC par rapport aux interfaces d'administration utilisées par le CSP. Les interfaces d'administration mises à la disposition du CSC ne doivent permettre aucune connexion avec les comptes d'administrateur relevant de la responsabilité du CSP. • Les interfaces d'administration utilisées par le CSP ne doivent pas être accessibles depuis un réseau public et ne doivent donc pas permettre de connexion des utilisateurs relevant de la responsabilité du CSC. Si des interfaces d'administration sont mises à disposition du CSC avec un accès via un réseau public, les flux d'administration doivent être authentifiés et chiffrés selon les exigences. • Mettre en œuvre un système d'authentification à deux facteurs pour l'accès : <ul style="list-style-type: none"> ○ aux interfaces d'administration utilisées par le CSP, ○ aux interfaces d'administration dédiées aux CSC. • Dans le cadre d'un service SaaS, les interfaces d'administration mises à disposition des CSC doivent être distinguées des interfaces destinées aux utilisateurs finaux. • Si une interface d'administration est accessible depuis un réseau public, le processus d'authentification doit avoir lieu avant toute interaction entre l'utilisateur et l'interface en question. 		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Interface d'administration 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

AID-9 	Le CSP doit fournir une procédure exigeant que les administrateurs se consacrent exclusivement à l'exécution des tâches administratives	
<p>Le CSP doit documenter et mettre en œuvre une procédure exigeant que les administrateurs sous sa responsabilité utilisent des terminaux dédiés à l'exécution exclusive des tâches administratives. Si le CSP autorise la mobilité des administrateurs sous sa responsabilité, il doit documenter cette autorisation dans une politique. La solution mise en œuvre doit garantir que le niveau de sécurité dans ce scénario de mobilité est au moins équivalent au niveau de sécurité en dehors du scénario de mobilité</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Procédure correspondante 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7


3.1.12 ACQUISITION, DÉVELOPEMENT ET MAINTENANCE DES SYSTÈMES D'INFORMATION

3.1.12.1 Analyse de code


DEV-1 	Le CSP fournit des développements exempts de fonctionnalités cachées	
<p>Les développements fournis par le CSP doivent uniquement effectuer les tâches et opérations pour lesquelles il existe une spécification écrite et ne doivent avoir aucune utilisation cachée.</p> <p>Le CSP s'engage à fournir des livrables exempts de tous éléments malveillants connus.</p> <p>Le CSP doit documenter et mettre en œuvre des mesures de détection, de prévention et de récupération pour se protéger contre les codes malveillants. Le champ d'application de cette exigence sur le système informatique du service doit inclure les postes utilisateurs dont le CSP est responsable et les flux entrants sur ce même système informatique.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Engagement du CSP dans le PAS 	<ul style="list-style-type: none"> • Vérification de l'engagement du CSP dans le PAS 	<ul style="list-style-type: none"> • 100% des développements exempts de fonctionnalités cachées • 100% des livrables exempts de fonctionnalités cachées

DEV-2 	Le CSP accepte la responsabilité de ses développements sur les activités du CSC	
<p>Le CSP doit garantir la sécurité des informations tout au long du cycle de développement des systèmes informatiques.</p> <p>Le CSP doit documenter et mettre en œuvre des règles pour le développement sécurisé de logiciels et de systèmes, et les appliquer aux développements internes.</p> <p>Le CSP doit documenter et mettre en œuvre une formation appropriée en développement sécurisé pour les employés concernés.</p> <p>Le CSP accepte la responsabilité civile et pénale des impacts des vulnérabilités ou des fonctionnalités cachées qui peuvent être présentes dans les livraisons, en raison de sa négligence ou de sa malveillance sur les activités du CSC.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Engagement du CSP dans le PAS 	<ul style="list-style-type: none"> Vérification de l'engagement du CSP dans le PAS 	<ul style="list-style-type: none"> Engagement présent dans PAS

3.1.12.2 API

DEV-3 	Le CSP doit sécuriser ses API	
<p>Le CSP s'engage à mettre en œuvre le niveau de sécurité requis pour sécuriser l'ensemble des APIs mises à disposition du CSC.</p> <p>Le CSP doit maintenir à jour ce niveau de sécurité.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Solution de sécurisation des APIs 	<ul style="list-style-type: none"> Contrôle par le CSC 	<ul style="list-style-type: none"> Solution validée par le CSC

3.1.13 SOUS-TRAITANCE

SUB-1 	Le CSP présente ses sous-traitants au CSC	
<p>Le CSP peut recourir à un sous-traitant, y compris pour effectuer des activités spécifiques de traitement de données personnelles. Le terme "sous-traitance" englobe toutes les activités réalisées</p>		

pour le compte du CSP par une société tierce (par exemple, développement, routage des e-mails, archivage, etc.).

Le CSP s'engage à obtenir l'autorisation écrite préalable et spécifique du CSC avant de recourir à la sous-traitance ou d'apporter toute modification concernant l'ajout ou le remplacement de tout sous-traitant. Ces informations doivent indiquer clairement les activités et les traitements sous-traités, les mesures techniques et organisationnelles prévues, l'identité et les coordonnées du sous-traitant, ainsi que les dates de sous-traitance.

Toutes les exigences applicables au CSP s'appliquent également à ses sous-traitants. Le CSP s'engage à mettre en œuvre et à surveiller le respect par ses sous-traitants des exigences contractées avec le CSC. Le CSP doit garantir la protection des informations auxquelles ses fournisseurs peuvent accéder, surveiller les services convenus et les exigences en matière de sécurité. Il incombe au CSP de veiller à ce que tout prestataire offre des garanties suffisantes concernant la mise en œuvre de mesures techniques et organisationnelles appropriées afin que le traitement des données personnelles respecte les exigences de la législation sur la protection des données. Si le prestataire ne respecte pas ses obligations en matière de protection des données, le CSP reste entièrement responsable envers le CSC de l'exécution des obligations de son prestataire.


Le CSP doit s'engager pour toute la durée du service, même s'il n'utilise pas la sous-traitance au début du service. Le CSP doit fournir une liste des identités, profils, domaine d'intervention et responsabilités de ses parties prenantes, y compris les sous-traitants, impliquées dans le service. Le CSP doit maintenir une liste à jour de tous les tiers impliqués dans la mise en œuvre du service, tels que les hébergeurs, les développeurs, les intégrateurs, les archivistes, les sous-traitants intervenant sur site ou à distance, les fournisseurs de climatisation, etc. Cette liste doit être exhaustive, préciser la contribution du tiers au service et au traitement des données personnelles, et prendre en compte les cas de sous-traitance à plusieurs niveaux. Cette liste doit être tenue à jour à mesure que le personnel impliqué dans le service change.


Pour maintenir le contrôle de la conformité avec le PSSI du CSC par les parties prenantes du CSP, le niveau de sous-traitance "cascadée" par le CSP ne doit pas dépasser "1" dans le cadre du service, c'est-à-dire CSP / Sous-traitant 1. Un exemple de sous-traitance "cascadée" interdite serait CSP / Sous-traitant 1 / Sous-traitant 2.

Le CSP doit exiger que les tiers impliqués dans la mise en œuvre du service maintiennent un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Cela doit se faire par le biais d'exigences adaptées à chaque tiers et à sa contribution au service, dans les spécifications ou dans les clauses de sécurité des accords de partenariat. Le CSP doit inclure ces exigences dans les contrats avec les tiers. Le CSP doit contracter des clauses d'audit avec chacun des tiers impliqués dans la mise en œuvre du service, permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent document de référence. Le CSP doit définir et attribuer des rôles et responsabilités pour la modification ou la résiliation de son contrat avec un tiers impliqué dans la mise en œuvre du service.


Enfin, dans le cadre du document de transparence précontractuelle, le CSP doit spécifier tous les processus mentionnant l'utilisation de sous-traitants lors de l'activité de portabilité des données.


<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Engagement du CSP dans le PAS Liste des identités, profils, périmètres d'intervention et responsabilités des intervenants du CSP 	<ul style="list-style-type: none"> Vérification de l'engagement du CSP dans le PAS Audit par le CSC 	<ul style="list-style-type: none"> 100% de conformité entre le contenu de la liste fournie et les vérifications réalisées par le CSC

SUB-2	Le CSP met en place des procédures pour surveiller les activités et les impacts du sous-traitant	
		
<p>Le CSP doit documenter et mettre en œuvre une procédure pour surveiller régulièrement les mesures mises en place par les tiers impliqués dans la mise en œuvre du service afin de répondre aux exigences du présent document de référence.</p> <p>Le CSP doit documenter et mettre en œuvre une procédure de suivi des modifications apportées par les tiers impliqués dans la mise en œuvre du service susceptibles d'affecter le niveau de sécurité du système informatique du service. Si une modification du tiers impliqué dans la mise en œuvre du service affecte le niveau de sécurité du service, le CSP doit informer immédiatement tous les CSC et mettre en œuvre des mesures pour rétablir le niveau de sécurité précédent.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Procédure de suivi des sous-traitants 	<ul style="list-style-type: none"> Réception par le CSC 	<ul style="list-style-type: none"> Validation par le CSC

SUB-3	Le CSP fournit des garanties vérifiées dans le cas où le CSP ou les sous-traitants sont soumis à des obligations légales extraterritoriales de transfert de données.	
		
<p>Dans le cas où le fournisseur ou le sous-traitant est soumis à des obligations légales de transmettre ou de divulguer des données sur la base d'une ordonnance légale non-UE, des garanties vérifiées doivent être mises en place pour garantir que toute demande d'accès est conforme au droit de l'UE.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Engagement du CSP dans le PAS 	<ul style="list-style-type: none"> Vérification de l'engagement du CSP dans le PAS 	<ul style="list-style-type: none"> Engagement du CSP dans le PAS

3.1.14 CONFORMITÉ

CMPL-1 	Engagement sur les données du CSP	
<p>Le contrat entre le CSP d'infrastructure et le CSC établit spécifiquement les rôles respectifs et les responsabilités partagées du CSP et du CSC en ce qui concerne la sécurité et la protection des données, ainsi que la configuration technique de l'environnement.</p> <p>Le CSP doit :</p> <ul style="list-style-type: none"> • garantir la confidentialité, l'intégrité et la disponibilité des données personnelles du responsable de traitement grâce à la mise en œuvre de mesures techniques et/ou organisationnelles appropriées. • garantir, avec des mesures appropriées, que le CSC a la possibilité de rectifier et de compléter lui-même les données personnelles incomplètes ou de le faire effectuer par le CSP. • garantir que le CSC a la possibilité de supprimer lui-même les données personnelles ou de les faire supprimer par le CSP. • informer le CSC des violations de données à caractère personnel et de leur étendue sans délai indu, en utilisant des mesures appropriées. <p>Le destinataire (CSP) doit informer l'expéditeur des données (CSC) de son éventuelle incapacité à se conformer aux clauses de protection standard, et ce dernier (le client) doit alors suspendre le transfert de données et/ou résilier le contrat avec le premier (le fournisseur).</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Engagement du CSP 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

CMPL-2 	Respect des principes RGPD	
<p>Principes RGPD</p> <p>Le CSP s'engage à respecter l'intégralité des principes du Règlement Général sur la Protection des données conformément à l'article 33.3 des Conditions Particulières d'Achats (CPA) associées au marché.</p> <p>Dans ce cadre, il décrit de manière exhaustive :</p> <ul style="list-style-type: none"> - l'ensemble des mesures de sécurité qu'il met en œuvre afin de se conformer à l'obligation de sécurité des données à caractère personnel traitées. - l'ensemble des moyens et processus qu'il met en œuvre afin de se conformer au principe de conservation limitée des données à caractère personnel traitées. 		

- lorsque c'est le cas, il décrit l'ensemble des mesures de sécurité qu'il met en œuvre afin d'assurer **la protection particulière** des données à caractère personnel sensibles traitées.
- l'ensemble des dispositifs présents au sein du service permettant **d'informer les personnes** de l'utilisation des données les concernant l'ensemble des processus et moyens mis en œuvre permettant le respect du droit des personnes

Le CSP s'engage à coopérer avec le CSC afin de faire respecter pleinement l'ensemble de ces principes.

Délégué à la Protection des Données

Le CSP s'engage à fournir au CSC l'identité ainsi que les coordonnées de son Délégué à la Protection des Données.

Registre de traitements

Le CSP tient un registre de traitements des données à caractère personnel qu'il met à jour régulièrement. Il transmet au CSC son registre de traitement relatifs aux données à caractère personnel du CSC sur demande.

Localisation de l'hébergement

Le CSP renseigne la liste des pays dans lesquels il est susceptible de transférer les données à caractère personnel du CSC.

Lorsque ces données sont susceptibles d'être transférées en dehors de l'Union Européenne ou de l'Espace Economique Européen, le CSP transmet au CSC les preuves de la mise en place de garanties appropriées qui encadrent ces transferts, qu'il s'agisse de Règles d'entreprises contraignantes ou de clauses contractuelles types de la Commission Européenne.


Dans tous les cas, le CSP ne peut transférer des données à caractère personnel vers un pays tiers ou une organisation internationale sans l'accord préalable et écrit du CSC.

Sous-traitance

Si le CSP a recours à de la sous-traitance, il devra alors satisfaire pleinement l'ensemble des exigences mentionnées dans la clause « sous-traitance ».

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Engagement du CSP dans le PAS • Registre de traitement des données du CSP • Coordonnées du Délégué à la Protection des Données du CSP • Localisation de l'hébergement des données à caractère personnel • Règles d'entreprise contraignantes ou 	<ul style="list-style-type: none"> • Présence de l'engagement du CSP dans le PAS • Audit organisationnel par le CSC 	<ul style="list-style-type: none"> • 100% des traitements sont conformes au Règlement Général de la Protection des Données

Conditions générales de contrat		
---------------------------------	--	--

CMPL-3 	Lorsque le CSC utilise des services cloud pour traiter des données à caractère personnel, le CSP agit en tant que sous-traitant et doit se conformer à toutes les obligations applicables en vertu du RGPD.
--	--

Lorsque le CSC utilise des services cloud pour traiter des données personnelles, le CSP agit en tant que sous-traitant et doit se conformer à toutes les obligations du RGPD. L'étendue de l'implication des sous-traitants dans le traitement des données personnelles est clairement définie, et des mesures de gestion appropriées doivent être mises en place. Ce traitement doit être formellement accepté par l'utilisateur du cloud au préalable, et la liste des sous-traitants impliqués à tous les niveaux doit être communiquée à l'utilisateur du cloud.

Le contrat juridiquement contraignant stipule que les données ne seront traitées que sur la base des instructions documentées du CSC. En cas de responsabilité conjointe pour le traitement entre le CSP et le CSC, le contrat doit être conforme à l'article 26 du RGPD. Cela comprend la communication de l'accord aux personnes concernées et la désignation d'un point de contact pour les personnes concernées.


La finalité et la durée du traitement doivent être décrites aussi spécifiquement que possible dans l'accord juridiquement contraignant lié à la commande. Le CSP ne traite les données personnelles de l'utilisateur du cloud que dans la mesure nécessaire pour atteindre les finalités spécifiées du traitement. Le CSP est expressément interdit de traiter les données personnelles des utilisateurs du cloud à des fins d'exploration de données, de profilage ou de marketing, et en général, d'accéder aux données personnelles du CSC, sauf si nécessaire pour la fourniture des services cloud.

Le CSP doit veiller à ce que le traitement des données personnelles du CSC soit effectué uniquement sur instruction du CSC conformément à l'accord de traitement. Le CSP doit fournir les moyens au CSC de fournir aux individus qui le demandent des informations sur le traitement de leurs données personnelles. Avec les moyens à sa disposition, le CSC peut envoyer une copie des données personnelles dans un format structuré, couramment utilisé et lisible par machine.

Le CSP doit s'assurer que ses sous-traitants n'agissent que sur la base d'un accord juridiquement contraignant conformément à l'accord entre le CSP et le CSC. Le CSP doit également s'assurer que le CSC a la possibilité de restreindre le traitement des données personnelles eux-mêmes, ou de faire mettre en œuvre la restriction par le CSP.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Engagement du CSP dans le PAS Registre de traitement des données du CSP 	<ul style="list-style-type: none"> Présence de l'engagement du CSP dans le PAS Audit organisationnel par le CSC 	<ul style="list-style-type: none"> 100% des traitements sont conformes au Règlement Général de la Protection des Données

<ul style="list-style-type: none"> • Coordonnées du Délégué à la Protection des Données du CSP • Localisation de l'hébergement des données à caractère personnel • Règles contraignantes pour les entreprises ou Clauses Contractuelles Types 		
--	--	--

CMPL-4 	Le CSP doit régulièrement faire évaluer sa conformité aux exigences de protection des données personnelles par un tiers indépendant et externe	
<p>Le CSP doit régulièrement faire évaluer sa conformité aux exigences de protection des données personnelles par un tiers indépendant et externe.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Engagement du CSC et preuve d'audit 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

CMPL-5	Le CSP fournit un outil pour évaluer la conformité	
<p>Le CSP fournit au CSC un outil pour analyser son parc de machines virtuelles, ses bases de données, etc. afin de vérifier les incohérences de conformité et de configurer les correctifs.</p> <p>Un système de rapport des évaluations est attendu. Le CSP fournit des normes de conformité et les surveille.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Outil d'Analyse et de Remédiation 	<ul style="list-style-type: none"> • Utilisation de l'outil par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7 • Validation par le CSC

CMPL-6	Le CSP est certifié sur l'hébergement des données de santé	
<p>Le CSP fournit les certifications d'Hébergement des données de Santé (HDS) sur les 5 niveaux définis.</p> <p>Le CSP est certifié à minima sur les 4 niveaux HDS.</p> <p>Le CSP est certifié "Hébergeur d'infrastructure physique".</p>		
Livable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Certification sur les données de santé 	<ul style="list-style-type: none"> • Réception de la certification du CSP 	<ul style="list-style-type: none"> • Certification à minima sur les 4 niveaux HDS

CMPL-7	Le CSP est certifié ISO 27001, ISO 27017 et ISO 27018	
Le CSP est certifié ISO 27001, ISO 27017 et ISO 27018.		
Livable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • ISO27001, ISO27017 and ISO27018 certifications 	<ul style="list-style-type: none"> • Réception de la certification du CSP 	<ul style="list-style-type: none"> • Validation de la réception

CMPL-8	Le CSP a défini une roadmap détaillée pour obtenir la certification SecNumcloud délivrée par l'ANSSI	
<p>Le CSP a défini une roadmap détaillée pour obtenir la certification SecNumcloud délivrée par l'ANSSI.</p> <p>Le CSP s'engage à obtenir la certification dans un délais maximal de 18 mois après la signature du contrat.</p>		
Livable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Roadmap de certification SecNumcloud 	<ul style="list-style-type: none"> • Reception by the CSP 	<ul style="list-style-type: none"> • Validation par le CSC • Délais pour obtenir la certification < 18 mois après la date de signature du contrat

3.1.15 SERVICES DE SÉCURITÉ

SECS-1	Le CSP fournit des services de Reverse Proxy
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p>	

Le CSP propose des services de **Reverse Proxy**.

Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de Reverse Proxy 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-2

Le CSP fournit des services de Web Application Firewall

Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.

L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.

Le CSP propose des services de **Web Application Firewall**.

Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de Web Application Firewall 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-3

Le CSP fournit des services de sonde de protection contre les intrusions

Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.

L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.

Le CSP propose des services de **sonde de protection contre les intrusions (IPS et IDS)**.

Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée via la place de marché par exemple. Dans ce cas, le CSC devra être informée de cette sous-traitance.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de sonde de protection contre les intrusions 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-4	Le CSP fournit des services de Firewall	
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP propose des services de Firewall.</p> <p>Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de Firewall 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-5	Le CSP fournit des services de Proxy web	
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP propose des services de Proxy web.</p>		

Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de Proxy web 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-6	Le CSP fournit des services d'Anti-DDoS	
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP propose des services d'Anti DDoS.</p> <p>Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services d'Anti-DDoS 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-7	Le CSP fournit des services de Bastion	
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP propose des services de Bastion d'administration.</p>		

Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.

Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Services de Bastion 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-8	Le CSP fournit des services de SIEM (<i>Security information management system</i>)	
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP propose des services de SIEM.</p> <p>Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Services de SIEM 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-9	Le CSP fournit des services d'antivirus	
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP propose des services d'antivirus pouvant être déployés sur les VM du CSC et propose des scans antivirus des espaces de stockage.</p>		

Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services d'antivirus 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-10	Le CSP fournit des services de répertoire de correctifs de sécurité	
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP propose des services de répertoire de correctifs de sécurité.</p> <p>Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de répertoire de correctifs de sécurité 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-11	Le CSP fournit des services d'Annuaire	
<p>Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.</p> <p>L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.</p> <p>Le CSP propose des services d'Annuaire.</p>		

Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services d'annuaire 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-12**Le CSP fournit des services de base de temps**

Le CSP fournit à travers son catalogue de services, des services de sécurité assurant la sécurisation des infrastructures et applications du CSC.

L'infrastructure et le système d'exploitation sont sous l'entière responsabilité du CSP, qui les exploite et les administre.

Le CSP propose des services **de base de temps**

Si certains services de sécurité ne peuvent pas être pris en charge directement par le CSP. Il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de base de temps 	<ul style="list-style-type: none"> Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de sécurité 	<ul style="list-style-type: none"> Disponibilité 24h/24, 7j/7

SECS-13**Le CSP permet au CSC de configurer ses services de sécurité**

Le CSP fournit à travers son catalogue de services, l'infrastructure et les logiciels nécessaires au déploiement des services de sécurité du CSC.

Liste de services de sécurité pouvant être apportés par le CSC :

- Reverse Proxy
- Sonde de protection contre les intrusions (IPS)
- Firewall
- Proxy web
- Bastion

- SIEM (security information management system)
- Antivirus
- Répertoire de correctifs de sécurité
- Annuaire
- Base de temps

Les services apportés par le CSC doivent être interopérables avec le cloud du CSP.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Services cloud de sécurité 	<ul style="list-style-type: none"> • Possibilité pour le CSC d'approvisionner, paramétrer et supprimer les plateformes applicatives proposées à travers les services de type PaaS 	<ul style="list-style-type: none"> • 100% Compatibilité


3.2 EXIGENCES DE SÉCURITÉ DE CONFIANCE


TRST-1	Le CSP doit informer le CSC de la possibilité d'accéder au service cloud via d'autres services cloud ou systèmes informatiques du CSC	
Le CSP doit informer le CSC de la possibilité d'accéder au service cloud via d'autres services cloud ou systèmes informatiques du CSC.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Liste des moyens et services permettant l'accès aux services cloud 	<ul style="list-style-type: none"> • Tests des différents moyens d'accès aux services cloud 	<ul style="list-style-type: none"> • Aucun tiers ou utilisateur externe ne devrait avoir la possibilité d'accéder au cloud.


TRST-2 	Propos complémentaire : Le service fourni par le CSP doit être conforme à la législation existante sur les droits fondamentaux et aux valeurs de l'Union européenne telles que le respect de la dignité humaine, de la liberté, de l'égalité, de la démocratie et de l'état de droit	
Le service fourni par le CSP doit être conforme à la législation existante sur les droits fondamentaux et aux valeurs de l'Union européenne telles que le respect de la dignité humaine, de la liberté, de l'égalité, de la démocratie et de l'état de droit. Il peut être pris en compte, pour l'évaluation de la		


conformité susmentionnée, le fait que le fournisseur entretienne des liens avec un gouvernement étranger ou un organisme public.

TRST-3	Le CSP doit spécifier les contrôles de sécurité utilisés lors de l'importation des données	
Le CSP doit spécifier les contrôles de sécurité (par exemple, les contrôles d'accès) utilisés lors de l'importation des données.		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Procédure d'importation des données 	<ul style="list-style-type: none"> • Réception des documents et tests par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC

TRST-4	Le CSP doit garantir une gestion appropriée des demandes d'investigation de l'État	
		
Le CSP doit garantir une gestion appropriée des demandes d'investigation de l'État		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Engagement du CSP dans le PAS 	<ul style="list-style-type: none"> • Contrôle de l'engagement du CSP présent dans le PAS 	<ul style="list-style-type: none"> • Engagement du CSP présent dans le PAS

TRST-5	Propos complémentaire : La compétence juridictionnelle pour tous les accords de service du CSP (avec le CSC ou avec ses sous-traitants) est exclusivement européenne	
		
La compétence juridictionnelle pour tous les accords de service du CSP (avec le CSC ou avec ses sous-traitants) est exclusivement européenne.		

<p>TRST-6</p> 	<p>Les actionnaires du CSP, dont le siège social et l'établissement principal ne sont pas établis dans un État membre de l'UE, ne peuvent pas, directement ou indirectement, individuellement ou collectivement, exercer un contrôle sur le CSP</p>	
<p>Les actionnaires du CSP, dont le siège social et l'établissement principal ne sont pas établis dans un État membre de l'UE, ne peuvent pas, directement ou indirectement, individuellement ou collectivement, exercer un contrôle sur le CSP. Le contrôle est défini comme la capacité d'une personne physique ou morale d'exercer une influence décisive directement ou indirectement sur le CSP par le biais d'une ou plusieurs entités intermédiaires, de jure ou de facto.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> Engagement du CSP dans le PAS Listes des principaux actionnaires non établis dans l'Union européenne 	<ul style="list-style-type: none"> Contrôle de l'engagement du CSP présent dans le PAS 	<ul style="list-style-type: none"> Engagement du CSP présent dans le PAS

<p>TRST-7</p> 	<p>Conformité avec l'article 48 du RGPD</p>	
<p>En cas de recours par le CSP, dans le cadre des services fournis au CSC, aux services d'une entreprise tierce - y compris un sous-traitant - dont le siège social, le siège et l'établissement principal sont situés en dehors de l'Union européenne ou qui est détenu ou contrôlé directement ou indirectement par une autre entreprise tierce enregistrée en dehors de l'Union européenne, ladite entreprise tierce ne doit avoir aucun accès aux données du CSC ni à la gestion des accès et des identités pour les services fournis au CSC. Cela inclut que le CSP, y compris l'un de ses sous-traitants, doit faire tout ce qui est possible dans le cadre de la juridiction pour refuser et minimiser l'impact de toute demande reçue des autorités non européennes visant à obtenir la communication de données personnelles relatives aux clients européens, sauf si la demande est faite dans le cadre de l'exécution d'un jugement ou d'une ordonnance de justice valide et légalement contraignante en vertu du droit de l'Union et du droit des États membres applicables, conformément à l'article 48 du RGPD.</p>		
<p>Livrable(s) :</p>	<p>Contrôle des résultats :</p>	<p>Niveau à atteindre :</p>
<ul style="list-style-type: none"> Engagement du CSP dans le PAS Liste des entreprises tiers ne faisant pas 	<ul style="list-style-type: none"> Control de l'engagement du CSP présent dans le PAS 	<ul style="list-style-type: none"> Engagement du CSP présent dans le PAS

partie de l'union européenne		
---------------------------------	--	--

4 CATALOGUE DE SERVICES D'INFRASTRUCTURE ET DE FONDATIONS

4.1 SERVICES D'INFRASTRUCTURE

4.1.1 PUISSANCE DE CALCUL

CSI-1	Le CSP met à disposition des services de <i>Compute</i>	
<p>Le CSP met à disposition du CSC des ressources informatiques lui permettant d'héberger ses applications.</p> <p>Parmi les services attendus et non limitatifs, le fournisseur devra décrire ce qu'il propose pour :</p> <ul style="list-style-type: none"> • La mise à disposition d'un catalogue de Machines virtuelles (dotées en CPU et RAM), • La mise à disposition de solutions permettant de partitionner un serveur en plusieurs, • La mise à disposition de solutions logicielles permettant d'ajuster les ressources en fonction des usages pour maintenir le niveau de performance attendu, • La mise à disposition de solution d'équilibrage ou de partage de charge pour optimiser les traitements, • La mise à disposition de service de conteneurisation pour distribuer les applications et normaliser la gestion de leur code, • La mise à disposition de solution pour automatiser des suites de commandes ou de traitement ; • La mise en place d'un socle qui permet aux développeurs de ne pas être astreints aux tâches de provisionnement et de maintien en conditions opérationnelles des infrastructures, • La mise à disposition de solutions permettant de mettre en place une architecture réactive aux événements, • La mise à disposition de capacités de calcul intégrant l'accélération graphique, • La mise à disposition de solutions permettant de monter une architecture de code serverless, • La mise à disposition de solutions de relevé de métriques sur site à l'aide de capteurs (IoT), • La mise à disposition d'outils de prédiction basés sur l'intelligence artificielle, • Le provisioning de machines sur le surplus du volume non utilisé à des coûts réduits. 		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Services de <i>compute</i> 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSI-2	Le CSP met à disposition des services de calcul haute performance	
<p>Le CSP met à disposition du CSC des services de calcul haute performance, consistant à utiliser le traitement parallèle pour exécuter des applications de façon efficace, fiable et rapide. LE CSC a également besoin de réseau rapide (e.g. infiniband) et de stockage parallèle.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Services de calcul haute performance 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

4.1.2 GESTION DES CONFIGURATIONS

CSI-3	Le CSP fournit un outil de gestion des configurations	
<p>Le CSP fournit au CSC une solution de gestion des configurations. Cette solution doit entre autres permettre d'utiliser la plateforme ou du code pour configurer les différents serveurs.</p> <p>LE CSC veut avoir la possibilité d'utiliser une solution tierce de gestion des configurations.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Outil de gestion des configurations 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSI-4	Le CSP fournit un outil de gestion des systèmes	
<p>Le CSP fournit au CSC un outil de gestion des systèmes présents dans le cloud public mais aussi dans l'environnement "on-prem" de l'ENTREPRISE. Parmi les services attendus, le CSC veut entre autres :</p> <ul style="list-style-type: none"> L'inventaire des ressources ; La version de l'OS déployé sur la machine ; Le statut des mises à jour/ patches et leurs gestions (pouvoir entre autre pousser des patches) ; La gestion des logs ; La gestion des créneaux de maintenances ; La gestion automatique des scripts et des créneaux de maintenance ; La gestion des créneaux d'accès en SSH ou RDP. 		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Outil de gestion des systèmes 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

4.1.3 STOCKAGE ET BACKUP

CSI-5	Le CSP met à disposition des services de stockage	
<p>Le CSP met à disposition du CSC des services d'enregistrement et de conservation (Stockage) de ses informations.</p> <p>Le CSP permet au CSC d'utiliser différents types de stockage :</p> <ul style="list-style-type: none"> • Stockage objet • Stockage en bloc • Stockage élastique (choix du dimensionnement du stockage à la demande en temps réel) • Stockage NFS • Archivage <p>Le stockage doit avoir des fonctions d'auto-tiering pour migrer automatiquement les données sur des espaces moins coûteux.</p> <p>Le CSP fournit également un système d'archivage et de versionning avec fonctions de tiering.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Services de stockage 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSI-6	Le CSP met à disposition des services de sauvegarde	
<p>Le CSP fournit au CSC des services de sauvegarde.</p> <p>Le CSP doit documenter et mettre en œuvre une politique de sauvegarde et de restauration des données dont il est responsable dans le cadre du service. Cette politique doit permettre une sauvegarde quotidienne de toutes les données (informations, logiciels, configurations, etc.) dont le CSP est responsable dans le cadre du service.</p> <p>Le CSP doit documenter et mettre en œuvre des mesures de protection des sauvegardes conformément à la politique de contrôle d'accès (voir chapitre dédié). Cette politique doit inclure une revue mensuelle des journaux d'accès aux sauvegardes.</p> <p>Le CSP doit documenter et mettre en œuvre une procédure de test régulier de la restauration des sauvegardes.</p> <p>Le CSP doit placer les sauvegardes à une distance suffisante des équipements principaux conformément aux résultats de l'évaluation des risques et afin de faire face aux grandes catastrophes. Les sauvegardes sont soumises aux mêmes exigences de localisation que les données opérationnelles.</p> <p>La communication entre le site principal et le site de sauvegarde doit être protégée par chiffrement, conformément aux exigences du chapitre correspondant.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Services de sauvegarde 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSI-7	Le CSP met à disposition un outil de snapshots	
<p>Le CSP met à disposition du CSC un outil permettant d'effectuer manuellement ou de manière automatique des sauvegardes (snapshot) des images de ses VMs et de ses bases de données. Le CSP fournit également un système de gestion des sauvegardes et du cycle de vie des images du CSC (registre privé).</p> <p>L'outil doit aussi offrir un système de déploiement des snapshots, de rollback et de restauration "point in time".</p>		
Livvable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Outil de snapshots 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

4.1.4 GESTION DES TEMPLATES ET RESSOURCES

CSI-8	Le CSP fournit des outils pour créer et stocker des <i>templates</i> de ressources	
<p>Le CSP fournit le CSC un outil permettant de créer des <i>templates</i> de ses serveurs, d'infra as code, d'API pour faciliter leurs créations.</p> <p>Le CSP permet au CSC de stocker les <i>templates</i> liés aux activités des opérations (OPS) dans des <i>templates</i> type yaml (déclaration des infrastructures, déclaration des pipelines etc.) et les stocker dans un outil de repository de code (protocole Git ou équivalent).</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livvable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Outils pour créer et stocker les <i>templates</i> de ressources 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

4.2 ADMINISTRATION RÉSEAUX

CSI-9	Le CSP fournit des outils pour gérer les équipements de gestion du réseau	
<p>Le CSP fournit aux CSC des outils pour configurer et gérer l'ensemble des fonctionnalités réseaux de l'environnement cloud du CSC dont :</p> <ul style="list-style-type: none"> • les VPC et les connecteurs ; • les sous-réseaux (publics et privés) ; • les droits d'accès (Sous réseaux, machines...) ; • les tables de routage ; 		

- les firewalls ;
- les DHCP ;
- les accès internet ;
- les équipements de sécurité (Firewall, proxy, reverse proxy, VPN, DNS public et privé, NAT ...)
- l'utilisation d'outils pour se connecter à d'autres VPC ;
- une passerelle dédiée pour l'échange entre les réseaux du CSP et du CSC ;
- des solutions privatives d'échanges réseaux avec le CSP.

Concernant les DNS, la solution du CSP devra permettre la délégation de domaines / zones DNS dont il est autoritaire pour ces dernières.

Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils pour gérer les équipements réseaux 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSI-10	Le CSP met à disposition une solution de routage dynamique	
<p>Le CSP met à disposition du CSC une solution de routage dynamique entre les environnements hébergés dans les data centers du CSC et les environnements cloud, tout en permettant au CSC d'avoir la maîtrise sur les tables de routage. Le protocole de routage dynamique BGP devra être supporté entre le client et le fournisseur. La solution de routage dynamique ne doit pas être couplée aux adresses IP privées du CSC afin de lever les contraintes liées à la réservation de plages IP interne du CSC.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Solution de routage dynamique 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

5 CATALOGUE DE SERVICES MÉTIERS

5.1 VALORISATION DES DONNÉES

5.1.1 BASES DE DONNÉES

CSM-1	Le CSP met à disposition des bases de données	
<p>Le CSP met à disposition du CSC des services de bases de données pour répondre à l'ensemble des besoins métiers tels que des bases de données relationnelles, OLTP, OLAP, NoSQL, Caching, graphe, scalable, etc...</p> <p>LE CSC souhaite disposer de bases de données pour collecter, ordonner, journaliser et stocker des informations provenant de bases de données opérationnelles et lui fournir ainsi un socle à l'aide à la décision.</p> <p>Des solutions ETL et workflow qui puissent être hébergées sur des VMs doivent aussi être disponibles.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de bases de données 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

5.1.2 COLLECTE ET TRAITEMENTS DES DONNÉES

CSM-2	Le CSP fournit des outils de collecte et de traitement des données
<p>Le CSP fournit au CSC des outils pour collecter de différentes sources et diffuser des données pour le traitement ordonné, incrémental et en temps réel.</p> <p>Le CSP fournit également au CSC des outils permettant de :</p> <ul style="list-style-type: none"> Convertir des données entrantes en un format commun Préparer les données pour l'analyse et la visualisation Migrer entre les bases de données Effectuer des synchronisations massives d'informations d'une source de données vers une autre. Partagez la logique de traitement des données sur les applications Web, les tâches par lots et les API Alimenter ses outils d'ingestion et d'intégration de données Consommer de gros fichiers XML, CSV et à largeur fixe Remplacer les tâches par lots par des données en temps réel <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interoperables avec le cloud du CSP pour répondre à ce besoin.</p>	

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de collecte et de traitement de données 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-3	Le CSP fournit des outils de <i>transcoding</i>	
<p>Le CSP fournit au CSC des outils pour changer le format de codage d'un média, pour compresser ou encapsuler un média audio ou vidéo dans un fichier, ou transporter un signal analogique ou numérique.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de transcoding 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-4	Le CSP fournit des outils de recherche et de modification de données	
<p>Le CSP fournit au CSC des outils permettant d'utiliser des requêtes SQL etc. afin de rechercher, ajouter, modifier, ou supprimer des données dans les bases de données relationnelles.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de recherche et de modification de données 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

5.1.3 ANALYSE ET RESTITUTION DES DONNÉES

CSM-5	Le CSP fournit des outils d'analyse de données
<p>Le CSP fournit au CSC des outils permettant :</p> <ul style="list-style-type: none"> D'analyser massivement des données à l'aide des framework de Big Data, tels que Spark, Hadoop... D'analyser en temps réel des données à l'aide de requêtes continues <p>Si des outils ne peuvent pas être fournis directement par le CSP, il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>	

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services d'analyse de données 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-6	Le CSP fournit des outils de modélisation et de restitution de données	
<p>Le CSP fournit au CSC des moyens, des outils et des méthodes lui permettant de modéliser et restituer ses données, dont la visualisation de type tableau. La visualisation des données devra être modulable à la volée.</p> <p>Le CSP met à disposition un outil de visualisation de données intégré en Saas pour :</p> <ul style="list-style-type: none"> Réaliser des restitutions graphiques (types de graphes différents utilisables), Exporter de gros volumes de données sous forme de listing Planifier les exports <p>LE CSC souhaite utiliser cet outil en interopérabilité avec Office 365.</p> <p>Si des outils ne peuvent pas être fournis directement par le CSP, il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra en être informée de cette sous-traitance.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de modélisation et de restitution de données 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

5.1.4 INTELLIGENCE ARTIFICIELLE

CSM-7	Le CSP fournit des outils de <i>machine learning</i> & <i>deep learning</i>	
<p>Le CSP fournit au CSC des outils pour concevoir, analyser, optimiser, développer et implémenter des méthodes d'apprentissage automatique pour ordinateurs, à partir de données afin d'améliorer leurs performances à résoudre des tâches.</p> <p>Le CSP met à disposition des <i>framework</i> de <i>deep learning</i> et des outils d'assistance virtuelle</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de <i>machine learning</i> <i>Framework</i> de <i>deep learning</i> Assistants virtuels 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-8	Le CSP fournit des outils de reconnaissance d'image	
<p>Le CSP fournit au CSC des outils pour la reconnaissance d'image.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de reconnaissance d'image 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-9	Le CSP fournit des outils de Text to Speech et Speech to Text	
<p>Le CSP fournit au CSC des outils pour créer une version sonore parlée du texte ou créer une version texte à partir d'une version sonore, dans un document informatique, comme un fichier d'aide ou une page Web.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de text to speech et speech to text 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-10	Le CSP fournit des outils d'interface conversationnelle	
<p>Le CSP fournit au CSC des programmes informatiques qui simulent la conversation humaine par le biais de commandes vocales ou de conversations textuelles ou les deux.</p> <p>Le CSP devra préciser si la technologie est basée sur du NLU (<i>natural language understanding</i>) et les langues prises en compte.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services d'interface conversationnelle 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

5.2 SERVICES DE MIGRATION

CSM-11	Le CSP fournit des outils de migration d'application	
<p>Le CSP fournit au CSC des outils d'aide à la migration des applications vers la plateforme du cloud provider.</p> <p>Si les outils ne peuvent pas être fournis directement par le CSP, il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour effectuer ces migrations.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de migration d'application 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-12	Le CSP fournit des outils de migration de bases de données	
<p>Le CSP fournit au CSC des outils pour migrer des bases de données hébergées dans n'importe quel type de plateforme vers le cloud public du provider.</p> <p>Ces migrations doivent pouvoir être effectuées "à froid" ou "à chaud".</p> <p>Si les outils ne peuvent pas être fournis directement par le CSP, il est possible de proposer une solution sous-traitée. Dans ce cas, le CSC devra être informée de cette sous-traitance.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces, interopérables avec le cloud du CSP, pour effectuer ces migrations.</p> <p>Le CSP fournit également au CSC des outils pour migrer des volumes importants de données (Exabyte Scale of Data) vers le cloud provider avec un impact restreint pour les utilisateurs.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de migration de bases de données 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-13	Le CSP fournit des outils de conversion de schéma source	
<p>Le CSP fournit au CSC des outils pour convertir les schémas sources des données et les objets dans un format compatible avec la base de données cible.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils ou services de conversion de schéma source 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-14	Le CSP fournit des outils de migration de serveur	
<p>Le TITUTLAIRE fournit au CSC des outils pour migrer des serveurs hébergés dans n'importe quel type de plateforme vers le cloud public du provider.</p> <p>Ces migrations doivent pouvoir être effectuées "à froid" ou "à chaud".</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour effectuer ces migrations.</p>		
Livvable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Outils ou services de migration de serveur 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

5.3 GESTION APPLICATIVE

5.3.1 DEVSECOPS

CSM-15	Le CSP fournit des outils de ressources intégrées et de gestion du déploiement	
<p>Le CSP fournit au CSC des outils permettant de préparer des environnements et de les déployer de manière automatique sur le cloud Public.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser une solution tierce interopérable avec le cloud du CSP pour effectuer ces actions.</p>		
Livvable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Outils de ressources intégrées et outils de gestion du déploiement 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-16	Le CSP fournit des outils d'analyse et de déblocage de code	
<p>Le CSP fournit au CSC des outils pour :</p> <ul style="list-style-type: none"> Revoir automatiquement le code produit par les développeurs (code applicatif ou code d'infrastructures) pour remonter les incohérences de code ou les écarts avec les normes de sécurité décidées par le RSSI ; Produire des rapports clairs et intelligibles pour assister à la remédiation, ajouter les actions de remédiation au backlog des développeurs. <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outil d'analyse et de déblocage 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-17	Le CSP fournit un outil de management de cycle de vie applicatif	
<p>Le CSP fournit au CSC un outil centralisé pour gérer le code source ainsi que les moyens nécessaires à la traçabilité du code et les users stories construites par les <i>products owners</i> :</p> <ul style="list-style-type: none"> • Rattachement du code livré aux tickets de développement, • Tag des commits, • Construction des packages déployés en production ... • Liens avec la documentation produite (design d'architecture ou commentaires de code ...) <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outil de management de cycle de vie applicatif 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-18	Le CSP fournit des outils de build et de tests	
<p>Le CSP fournit au CSC des outils pour :</p> <ul style="list-style-type: none"> • Builder le code produit par les développeurs en une version complète et cohérente exécutable sur un environnement (prod ou non prod) • Exécuter automatiquement les tests nécessaires à la validation de qualité du code et de la sécurité (tests unitaires, tests fonctionnels, analyse du code, tests de perf, tests de sécurité ...) <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud pour répondre à ce besoin</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Build & Test Tools 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-19	Le CSP fournit des outils de conteneurisation	
<p>Le CSP fournit au CSC des outils pour :</p> <ul style="list-style-type: none"> • Séparer les différents services d'une application en éléments d'infrastructures isolés, atomiques (légers et facilement remplaçables) 		

- Favoriser le scaling horizontal automatique des ressources pour permettre aux services d'absorber plus de charge en cas de besoins clients.

LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interoperables avec le cloud du CSP pour répondre à ce besoin.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils de conteneurisation 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-20 Le CSP fournit des outils de management de ressources DevOps

Le CSP permet au CSC d'appliquer aux ressources des équipes d'opérations (infrastructure as code, templates de pipelines) les mêmes standards que pour le code applicatif : ALM, CI/CD, testing automatisé, build etc.

Il doit spécifier quelles technologies sont interoperables avec l'environnement DevOps qu'il peut fournir ou avec d'autres environnements et normes du marché (par exemple, GitHub, Terraform...).

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils de management de ressources DevOps • Documentation de l'environnement 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-21 Le CSP fournit des outils de déploiement continu

Le CSP fournit au CSC des outils pour :

- Permettre aux développeurs de déployer automatiquement leur code sur les environnements de non-production à partir du moment où le code a été validé avant l'intégration et testé automatiquement par les outils de build et de tests automatiques ;
- Permettre au release manager, le cas échéant de déployer automatique en production après que les validations internes pertinents ont été réalisées ;
- Permettre un roll back automatique par le même biais, en cas d'incident en production impactant le bon fonctionnement de l'application.

LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interoperables avec le cloud du CSP pour répondre à ce besoin.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils de déploiement continu 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-22	Le CSP fournit des outils de Tests de Non-Régression	
<p>Le CSP fournit au CSC des outils pouvoir réaliser des Tests de Non-Régression (TNR) afin de s'assurer que les modifications et évolutions effectuées par les développeurs lors du dernier sprint n'ont pas entraîné d'effet de bord, en altérant les parties du code non modifiées. Ils doivent être lancés à chaque livraison.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils de tests de non-régression 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-23	Le CSP fournit des outils d'infrastructure as Code	
<p>Le CSP fournit au CSC un ensemble d'outils permettant de gérer, par des fichiers descripteurs ou des scripts, une infrastructure virtuelle. Cela permet de pouvoir gérer une infrastructure à part entière, de l'instance au réseau, incluant entre autres la gestion du DNS, du Load-Balancing, des sous-réseaux et des groupes de sécurité.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils d'infrastructure as code 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-24	Le CSP fournit des outils d'intégration continue	
<p>Le CSP fournit au CSC des outils pour :</p> <ul style="list-style-type: none"> • Stocker et versionner le code dans un repository accessible à tous (protocole Git ou équivalent) ; • Permettre aux développeurs de soumettre en confiance leur code et permettre une validation (pull request / peer review) par d'autres développeurs ou leur technical lead ; • Merger automatiquement ce code aux branches correspondantes et le cas échéant déclencher un processus de test automatiques via des triggers. <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils d'intégration continue 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-25	Le CSP fournit des outils de gestion des artefacts	
<p>Le CSP fournit au CSC des outils pour :</p> <ul style="list-style-type: none"> • Stocker les résultats des builds dans un outil permettant le versionning et le retour arrière automatique • Permettre la rotation automatique des artefacts out of date. <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Outils de gestion des artefacts 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-26	Le CSP fournit des outils d'interopérabilité	
<p>Le CSP fournit au CSC des outils pour :</p> <ul style="list-style-type: none"> • Déployer des infrastructures et par extension du code sur plusieurs providers de cloud publics ; • Monitorer des ressources déployées chez des opérateurs de cloud différent ; • Piloter le finops de ces ressources ; • Piloter le gestionnaire de ressources depuis l'environnement du CSC. <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Outils d'interopérabilité 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

5.3.2 SERVICES DE CONTENU

CSM-27	Le CSP fournit des outils de Content Delivery Network (CDN)	
<p>Le CSP fournit au CSC des outils de CDN pour lui permettre de réduire les temps de chargement et d'économiser la bande passante consommée.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Outils de Content Delivery Network 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-28	Le CSP fournit des outils de streaming	
Le CSP fournit au CSC une solution de streaming à la demande et en direct.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils de streaming 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/5

5.3.3 SERVICES APPLICATIFS

CSM-29	Le CSP fournit des systèmes de gestion de contenu	
Le CSP met à disposition du CSC des logiciels pour la conception et la mise à jour dynamique de sites Web ou d'applications multimédia (collaboration, structuration, publication, versionning de contenu)		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Systèmes ou logiciels de gestion de contenu 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-30	Le CSP fournit des services de Block Chain	
Le CSP fournit au CSC des fonctionnalités et des services en relation avec la Block-Chain. LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces pour répondre à ce besoin.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de Block Chain 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-31	Le CSP fournit des services de réalité virtuelle et réalité augmentée	
Le CSP fournit au CSC des fonctionnalités et des services en relation avec la réalité virtuelle et la réalité augmentée. LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Services de réalité virtuelle et de réalité augmentée 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-32	Le CSP fournit des outils SDKs (<i>software development kit</i>)	
<p>Le CSP met à disposition du CSC un ensemble d'outils logiciels destinés aux développeurs, facilitant le développement d'un logiciel sur une plateforme donnée.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Kit de développement logiciel 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-33	Le CSP fournit des services d'Edge computing	
<p>Le CSP fournit au CSC des services de <i>Edge computing</i>.</p> <p>LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Services d'Edge computing 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-34	Le CSP fournit des outils de files d'attente et de notifications	
<p>Le CSP met à disposition du CSC, la technique de file d'attente de messages, utilisée pour la communication interprocessus ou la communication de serveur-à-serveur.</p> <p>Elle permet le fonctionnement des liaisons asynchrones normalisées entre deux serveurs, c'est-à-dire de canaux de communications tels que l'expéditeur et le récepteur du message ne sont pas contraints de s'attendre l'un l'autre, mais poursuivent chacun l'exécution de leurs tâches. Le CSC souhaite également utiliser le principe de notifications pour implémenter des architectures réactives qui ne se synchronisent pas.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Outils de files d'attente et de notifications 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-35	Le CSP fournit un outil de recherche	
<p>Le CSP met à disposition du CSC des fonctionnalités de recherche rapides et hautement évolutives dans ses applications.</p>		

LE CSC souhaite également pouvoir indexer et rechercher des données de type document.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outil de recherche 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-36**Le CSP fournit des outils de workflow**

Le CSP fournit au CSC des outils de workflow pour :

- Coordonner les étapes de traitement entre les systèmes distribués ;
- Gérer des flux de travail, y compris l'état, les décisions, l'exécution des tâches et l'enregistrement ;
- Veiller à ce que les tâches soient exécutées de manière fiable, dans l'ordre et sans duplication.

Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils de workflow 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-37**Le CSP fournit des outils de notifications ciblées**

Le CSP fournit au CSC des outils de notifications ciblées pour :

- Configurer, exploiter et envoyer des notifications ciblées (vers des applications, par mail, sms)
- Publier des messages à partir d'une application et les transmettre aux utilisateurs ou à d'autres applications
- Envoyer des messages vers les appareils mobiles

Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils de notifications ciblées 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-38**Le CSP fournit des outils de gestion des API**

Le CSP fournit au CSC un outil de gestion des API pour :

- Gérer les workflows de développement et les droits d'accès ;
- Construire, publier et gérer des APIs pour renforcer la sécurité, assurer l'évolutivité et la haute disponibilité des micro-services.

LE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils de gestion des API 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

5.4 INTERNET DES OBJETS

CSM-39	Le CSP fournit des solutions d'Integrated Devices et Edge Systems	
Le CSP met à disposition du CSC des solutions d'Integrated Devices et Edge Systems.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Solutions d'Integrated Devices et Edge 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-40	Le CSP fournit des Device Gateway	
Le CSP met à disposition du CSC des passerelles pour connecter des appareils à son réseau.		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Solutions de Device Gateway 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-41	Le CSP fournit des outils de Device Management	
Le CSP fournit au CSC des outils pour visualiser et contrôler le matériel relié à l'ordinateur. Le CSC souhaite stocker et récupérer les informations d'état actuelles pour un appareil. Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> Outils de Device Management 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-42	Le CSP fournit des outils de calcul local	
Le CSP fournit au CSC des outils permettant d'exécuter automatiquement du code en langue Python au niveau de l'objet connecté. Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin		

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils de local compute 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-43	Le CSP fournit des bases de registre	
<p>Le CSP met à disposition du CSC des bases de registre (base de données utilisée par le système d'exploitation) pour contenir les données de configuration du système d'exploitation et des autres logiciels installés désirant s'en servir.</p> <p>eE CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Bases de registre 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-44	Le CSP fournit des moteurs de règles métier	
<p>Le CSP met à disposition du CSC des moteurs de règles métier afin de définir, tester, exécuter et maintenir séparément ses politiques d'entreprise et d'autres décisions opérationnelles du code d'application.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Solutions de moteurs de règles métier 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

5.5 SERVICES MOBILES

CSM-45	Le CSP met à disposition une solution d'identité mobile	
<p>Le CSP met à disposition du CSC une solution d'identité mobile qui permet :</p> <ul style="list-style-type: none"> • L'authentification juridique et la signature de transactions pour les services bancaires en ligne, • La confirmation des paiements, l'utilisation des services d'entreprise et la consommation de contenu en ligne. <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Solution d'identité mobile 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-46	Le CSP fournit des outils d'analyse de données mobiles	
<p>Le CSP met à disposition du CSC des outils pour mesurer et analyser les données produites par les applications et sites mobiles.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils d'analyse de données mobiles 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-47	Le CSP met à disposition des outils de tests d'applications mobiles	
<p>Le CSP met à disposition du CSC des outils (banc de tests) permettant d'évaluer ses applications mobiles pour tester les parcours, les fonctionnalités, les performances, etc...</p> <p>Les tests devront pouvoir être exécutés manuellement ou automatiquement grâce à des outils de la plateforme ou des standards du marché.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils de tests d'applications mobiles 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-48	Le CSP met à disposition une console de solutions intégrées	
<p>Le CSP met à disposition du CSC une console de solutions intégrées de type Sandbox permettant aux développeurs d'avoir une boîte à outils et de tester leurs codes ou leurs applications sur différents OS mobiles simultanément.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Console de solutions intégrées 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-49	Le CSP met à disposition des outils de synchronisation	
<p>Le CSP met à disposition du CSC des outils pour synchroniser automatiquement ses données cloud lors du passage d'un support à un autre (ordinateur vers mobile par exemple) par identification.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Outils de synchronisation 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-50	Le CSP met à disposition des outils de Mobile Device Management	
<p>Le CSP met à disposition du CSC des outils pour gérer sa flotte d'appareils mobiles, qu'il s'agisse de tablettes, de smartphones, d'ordinateurs portables, de capteurs ou autres objets. Cette gestion est effectuée au niveau du service informatique de l'organisation.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Outils de Mobile Device Management 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

CSM-51	Le CSP met à disposition une solution de backend mobile	
<p>Le CSP met à disposition du CSC une solution pour implémenter et industrialiser des Backend Mobile au sein de la plateforme cloud pour simplifier le développement d'applications mobiles.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interopérables avec le cloud du CSP pour répondre à ce besoin.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> Solution de backend mobile 	<ul style="list-style-type: none"> Réception et tests par le CSC 	<ul style="list-style-type: none"> Disponibilité 24/7

5.6 SERVICES ENTREPRISE

CSM-52	Le CSP met à disposition des outils de Virtual Desktop Infrastructure	
<p>Le CSP met à disposition du CSC des outils pour créer et gérer des bureaux virtuels avec ou sans accélération 3D pour ses utilisateurs, intégrés au VPC et au service d'annuaire.</p>		

Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interoperables avec le cloud du CSP pour répondre à ce besoin.

<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outils de Virtual Desktop Infrastructure 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

CSM-53	Le CSP met à disposition une solution de stockage et de partage documentaire	
<p>Le CSP met à disposition du CSC une solution pour stocker et partager des documents, avec fonctionnalité de flux de validation, intégrée au répertoire du CSC et compatible avec les ordinateurs de bureau, les ordinateurs portables, les tablettes et l'espace de travail.</p> <p>Le CSC souhaite avoir la possibilité d'utiliser des solutions tierces interoperables avec le cloud du CSP pour répondre à ce besoin.</p>		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Solution de stockage et de partage documentaire 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/7

5.7 SERVICES FINOPS

FIN-1	Le CSP met à disposition un outil de gestion des coûts	
<p>Le CSP fournit au CSC un outil lui permettant de gérer ses coûts. Cet outil doit permettre au CSP de :</p> <ul style="list-style-type: none"> • Suivre les coûts des différents services en filtrant par balise, services et régions ; • Extraire les données aux formats Excel, CSV ou PowerBI ; • Créer des tableaux de bord résumant les coûts financiers des différents services. Le CSC souhaiterait avoir la possibilité d'utiliser des solutions externes compatibles avec les services cloud du CSP pour répondre à cette exigence. 		
<i>Livrable(s) :</i>	<i>Contrôle des résultats :</i>	<i>Niveau à atteindre :</i>
<ul style="list-style-type: none"> • Outil de FinOps 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Disponibilité 24/5

6 FOCUS ENVIRONNEMENTAL

6.1 EXIGENCES ÉNERGÉTIQUES

NRG-1	Le CSP met en œuvre des mesures énergétiques	
<p>Niveau 1 (Mesure) :</p> <p>Les fournisseurs de services cloud fournissent à leurs clients des données sur l'efficacité énergétique de leurs centres de données en utilisant la méthode de calcul présentée dans la norme ISO IEC 30134-2 sur le PUE, sur le coefficient d'énergie verte (GEC) et sur le facteur de réutilisation de l'énergie (ERG).</p> <p>Niveau 2 (Actions) :</p> <p>Le mix énergétique de génération d'électricité utilisé par les réseaux qui alimentent les centres de données des fournisseurs de services cloud garantit un facteur d'émission de moins de 100gCO₂ eq / kWh. Spécifiez les règles de calcul.</p> <p>Les centres de données des fournisseurs de services cloud doivent respecter des normes élevées d'efficacité énergétique, conformément à l'ISO 30134-2 et en enregistrant l'infrastructure utilisée par le fournisseur auprès du Code de conduite de l'UE pour l'efficacité énergétique dans les centres de données. Les centres de données fonctionnant à pleine capacité doivent atteindre un objectif de PUE annuel d'ici 2030 de :</p> <ul style="list-style-type: none"> • 1,2 ou moins dans les régions climatiques tempérées (climats arctique, subarctique et tempéré) ; • 1,3 ou moins dans les régions climatiques chaudes (climats subtropical, tropical et équatorial). <p>Niveau 3 (Certifications) :</p> <p>Les fournisseurs de services cloud démontrent leur conformité à l'ISO 50001 (mise en place d'un système de gestion de l'énergie).</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • PUE • GEC • ERG • <i>Datacenters emissions factor</i> • Certification ISO 50001 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC des niveaux 1, 2 ou 3

6.2 ÉMISSIONS ET EMPREINTE CARBONE

CRB-1	Le CSP met en œuvre des mesures de réductions des ses émissions et de son empreinte carbone	
<p>Niveau 1 (Mesure) :</p> <p>Les fournisseurs de services cloud fournissent à leurs clients des données sur l'efficacité carbone de leurs centres de données en utilisant la méthode de calcul présentée dans la norme ISO IEC 30134-2, le CUE (Efficacité d'Utilisation du Carbone).</p> <p>Les fournisseurs de services cloud doivent divulguer l'emplacement géographique de leurs émissions (Émissions Basées sur la Localisation) ainsi que les types de marchés d'énergie renouvelable ou à faible émission de carbone qu'ils utilisent.</p> <p>Le CSP devrait fournir tous les détails sur les politiques de compensation carbone et comment cela pourrait affecter les différents indicateurs et mesures environnementaux.</p> <p>Niveau 2 (Actions) :</p> <p>De la part du CSP :</p> <p>Les fournisseurs de services cloud rapportent de manière transparente leurs données des scopes 1, 2 et 3 avec une publication de la méthodologie complète, incluant la définition des scopes, pour l'ensemble du cycle de vie des centres de données et pour chacun des sites, et en dehors de la stratégie de compensation carbone.</p> <p>Les fournisseurs de services cloud doivent spécifier toutes les hypothèses qui leur permettent de calculer leur empreinte environnementale sur les scopes 1, 2 et 3 (concernant les gaz à effet de serre), l'épuisement des ressources abiotiques non renouvelables (minérales et fossiles), l'impact sur les ressources en eau et sur l'énergie primaire non renouvelable.</p> <p>Les fournisseurs de services cloud expliquent les différents mécanismes de compensation carbone utilisés pour réduire l'empreinte carbone de leurs activités cloud et spécifient la trajectoire de réduction prévue.</p> <p>Pour le CSC :</p> <p>Les fournisseurs de services cloud offrent à leurs clients un outil leur permettant de mesurer leur impact carbone par compte (abonnement, projet, etc.), par service et par région de cloud computing.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • CUE • Scope 1,2 et 3 • Outil de mesure d'impact carbone 	<ul style="list-style-type: none"> • Réception et tests par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC des niveaux 1, 2

6.3 EXIGENCES DE RESSOURCES HYDRIQUE ET RÉCUPÉRATION DE LA CHALEUR

WAT-1	Le CSP met en œuvre des mesures d'économie d'eau	
<p>Niveau 1 (Mesure) : Les fournisseurs de services de cloud computing rapportent leurs objectifs annuels d'efficacité de l'utilisation de l'eau (WUE) pour chacun de leurs centres de données.</p> <p>Niveau 2 (Actions) : Les fournisseurs de services cloud doivent détailler leur impact sur les ressources en eau nécessaires au fonctionnement de leurs centres de données, en précisant les volumes prélevés, rejetés et consommés, ainsi que le type d'eau impliqué (rivières, eau potable, eau de mer, eaux grises, eaux usées, etc.). Les fournisseurs doivent également préciser les résultats de l'efficacité de l'utilisation de l'eau obtenus.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • WUE • Analyse d'impact 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC des niveaux 1, 2

HT-1	Le CSP met en œuvre des mesures d'optimisation de la chaleur	
<p>Niveau 1 (Mesure): Les fournisseurs de services cloud indiquent quelle technique de refroidissement et de traitement de l'air est utilisée dans leurs centres de données (refroidissement gratuit, refroidissement à basse température, etc.). Les fournisseurs précisent le point de consigne de température dans le centre de données, mesuré au point de récupération, c'est-à-dire en aval des serveurs.</p> <p>Niveau 2 (Actions): Les fournisseurs de services cloud récupèrent la chaleur perdue de leurs centres de données chaque fois que possible.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Technique de refroidissement et de traitement de l'air • Point de consigne de température • Analyse de la chaleur perdue 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC des niveaux 1 ou 2

6.4 EXIGENCES SUR LE CYCLE DE VIE DES COMPOSANTS ÉLECTRONIQUES

LFC-1	Le CSP met en œuvre des mesures d'optimisation du cycle de vie des composants électroniques	
<p>Les fournisseurs de services cloud s'engagent à respecter au moins la législation sur le recyclage des équipements électriques et électroniques (DEEE).</p> <p>Niveau 1 (Mesure) :</p> <p>Les fournisseurs de services cloud communiquent sur l'impact, au moins carbone et de préférence multi-critères, de l'ensemble du cycle de vie de leurs infrastructures (datacenters, serveurs, réseaux, etc.).</p> <p>Les fournisseurs de services cloud doivent communiquer leur politique en matière d'approvisionnement, de durée de vie moyenne, de recyclage et de remise à neuf du matériel informatique intégré dans leurs datacenters et équipements informatiques (serveurs et équipements réseau) et sur leurs pratiques liées à l'économie circulaire.</p> <p>Niveau 2 (Actions) :</p> <p>Les fournisseurs de services cloud s'engagent à communiquer des informations sur la durée de vie de leur équipement et de leurs serveurs d'ici 2025.</p> <p>Les fournisseurs de services cloud communiquent à chacun de leurs clients leurs objectifs numériques pour le pourcentage d'équipements et de serveurs réparés, recyclés ou réutilisés d'ici 2025.</p> <p>Les fournisseurs de services cloud s'engagent à promouvoir la réutilisation à 100 %, la réparation ou le recyclage de leur équipement et de leurs serveurs usagés.</p> <p>Niveau 3 (Certifications) :</p> <p>Les fournisseurs de services cloud démontrent leur conformité à la norme ISO 140001 (gestion de l'impact environnemental).</p> <p>Les fournisseurs de services cloud se conforment à la norme ISO 14069 sur la quantification des gaz à effet de serre, et suivent la "Norme méthodologique pour l'évaluation environnementale des services d'hébergement informatique en datacenter et des services cloud" de l'ADEME.</p> <p>Les composants des datacenters des fournisseurs de services cloud respectent les normes d'éco-conception. Le CSP doit indiquer quelles normes/références sont suivies.</p>		
Livrable(s) :	Contrôle des résultats :	Niveau à atteindre :
<ul style="list-style-type: none"> • Indicateurs sur les hardwares • Certifications 	<ul style="list-style-type: none"> • Réception par le CSC 	<ul style="list-style-type: none"> • Validation par le CSC des niveaux 1, 2 ou 3

À PROPOS DU CIGREF

Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

Appartenance

Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

Intelligence

Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

Influence

Le Cigref fait connaître et respecter les intérêts légitimes de ses entreprises membres. Instance indépendante d'échange et de production entre praticiens et acteurs, Il est une référence reconnue par tout son écosystème.

**NOUS
CONTACTER**

www.Cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
Cigref@Cigref.fr



Cigref
RÉUSSIR
LE NUMÉRIQUE