Achat de cloud par le secteur public

Manuel - Comprenant des exemples de clauses d'appels d'offres

Mentions légales

Ce document est fourni à titre informatif uniquement. Il n'a pas été développé conformément aux exigences légales concernant les passations de marchés publics dans une région en particulier. Il incombe aux clients cloud de procéder à leur propre évaluation indépendante des informations contenues dans ce document. Chaque client est également responsable de l'usage qu'il fait des produits ou services d'un fournisseur de cloud. Ce document ne crée pas de garanties, représentations, engagements contractuels, conditions ni assurances.

Les exemples de clauses ne doivent pas être interprétés comme des avis ou conseils juridiques. Les clients cloud doivent consulter leurs propres conseillers juridiques au sujet de leurs responsabilités en vertu de la loi applicable dans le pays où ils mènent leurs opérations. CISPE décline expressément toute garantie, responsabilité ou tout dommage associé aux ou découlant des informations fournies dans le présent document.

À propos du CISPE

CISPE (*Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) est une coalition industrielle indépendante à but non lucratif. Nous représentons les fournisseurs de service d'infrastructure de cloud en Europe et travaillons avec le secteur et les responsables politiques pour conseiller et donner des formations sur les services de cloud et leur rôle dans le secteur, la vie publique et la société en général.

Nos membres, dont le nombre est en augmentation constante, comprennent des entreprises menant leurs opérations dans tous les pays de l'UE et dont les sièges sociaux sont situés dans 16 pays européens. L'association est ouverte aux entreprises à condition qu'elles déclarent qu'au moins un de leurs services répond aux exigences du Code de conduite de protection des données du CISPE. Nous :

- Défendons les avantages des politiques de passation de marché public donnant la priorité au cloud dans l'UE et ses États membres
- Soutenons des exigences de sécurité et des normes techniques cohérentes à l'échelle de l'UE
- Respectons des exigences de confidentialité exhaustives avec un Code de conduite
- Œuvrons à la conservation de l'ouverture, de la compétitivité et du non-enfermement du marché de l'infrastructure de cloud dans l'UE
- Empêchons les obligations de supervision de contenu injustifiées dans le cadre juridique de l'UE

Nos membres fournissent et maintiennent les principaux « blocs de construction informatiques » grâce auxquels le gouvernement, les autorités publiques et les entreprises peuvent créer leurs propres systèmes et fournir des services essentiels à des milliards de citoyens. Dans cette optique, nous favorisons le développement de technologies et services de pointe intégrant l'intelligence artificielle (IA), les objets connectés, les véhicules autonomes et la 5G, ainsi que la nouvelle génération de technologie de connectivité cellulaire.

Code de conduite relatif aux services d'infrastructure de cloud

Le code de conduite CISPE a précédé l'entrée en vigueur du Règlement général sur la protection des données (RGPD). Il s'aligne sur les exigences strictes du RGPD pour aider les fournisseurs d'infrastructure de cloud à ainsi respecter et offrir un cadre solide, permettant aux clients de choisir des fournisseurs de cloud et de compter sur leurs services. Plus de 100 services sont déclarés dans le Code de conduite CISPE, fournis par plus de 30 entreprises basées dans plus de 16 États membres de l'UE et utilisés par des millions d'utilisateurs finaux et de consommateurs. https://cispe.cloud/code-of-conduct/

CISPE et le secteur public

CISPE contribue au débat sur la politique publique européenne et œuvre pour assurer une meilleure compréhension du rôle, de la participation et du potentiel du secteur de l'infrastructure de cloud en Europe.
Le modèle d'achat public doit conditionner le processus d'adoption et d'utilisation du cloud computing, mais l'acquisition de services de cloud diffère de la plupart des acquisitions de technologies traditionnelles que connaît le secteur public. Les approches d'approvisionnement doivent être repensées : CISPE encourage les décideurs de l'UE à développer une approche plus ambitieuse et tournée vers l'avenir à l'échelle de l'UE, en s'appuyant sur des initiatives de politique « cloud first », qui favorisent la croissance du marché de l'infrastructure de cloud unique en Europe et les objectifs de croissance du Marché unique numérique (MUN) qui les sous-tendent.

Le but de ce manuel est de fournir des conseils et un support aux autorités publiques pour l'acquisition de services de cloud.

En savoir plus
Membres du CISPE : https://cispe.cloud/members
Comité exécutif : https://cispe.cloud/board-of-directors
Services de cloud computing déclarés selon le Code de conduite CISPE : https://cispe.cloud/publicregister

Table des matières

v 2020 05 11

Résumé et objectif de ce manuel

L'objectif de ce **Manuel d'achat de services de cloud** est de fournir des conseils aux clients cloud qui souhaitent acheter des services de cloud grâce à un processus d'acquisition compétitif (**Appel d'offres de services de cloud - AO**), mais qui n'ont pas l'expérience nécessaire pour créer un accord-cadre de cloud.

Ce document est fourni à titre informatif uniquement. Il n'a pas été développé conformément aux exigences légales concernant les passations de marchés publics dans une région ou un pays en particulier.

Le manuel se penche également sur les critères de sélection supplémentaires pour les **contrats exécutoires** ou **mini compétitions** lors de l'achat d'un accord-cadre de cloud. Les sections du manuel sont organisées de la même façon qu'un AO informatique générique. Les exemples d'AO générique et de texte de critères de sélection sont accompagnés d'une explication aidant à comprendre pourquoi un AO de cloud est différent d'un AO informatique traditionnel.

> ***« Services de cloud »*** *désigne toutes les technologies cloud et les services associés auxquels un utilisateur final peut avoir besoin d'accéder. Cela inclut le consulting ou les services professionnels/managés nécessaires pour soutenir et exécuter la migration vers le cloud et soutenir les charges de travail dans le cloud, en plus de l'infrastructure de cloud elle-même et les services de marketplace de cloud tels que les produits Logiciels en tant que service (SaaS).*

L'émergence du cloud computing en tant que choix par défaut pour l'informatique du secteur public est l'occasion de moderniser les stratégies d'approvisionnement existantes. Les processus d'acquisition axés sur le cloud peuvent permettre à des entités du secteur public de bénéficier de tous les avantages du cloud, comme l'accès à une innovation de pointe, une vitesse et une capacité d'adaptation supérieures, une sécurité et une gestion de la conformité améliorées, tout en atteignant efficacité et réduction des coûts.

Les méthodes d'approvisionnement informatique traditionnelles pour l'achat de matériel, de logiciels et de Datacenters ne s'appliquent pas à l'achat de services de cloud. Les approches de la tarification, de la gouvernance de contrat, des conditions générales, de la sécurité, des exigences techniques, des contrats de niveau de service, etc. sont différentes dans un modèle de cloud. L'utilisation de méthodes d'approvisionnement existantes réduit ou élimine les avantages fournis par le cloud.

L'un des meilleurs moyens d'acquérir efficacement des services de cloud pour le secteur public consiste à passer par un **accord-cadre de cloud**, une attribution multi-organisationnelle d'un menu de clouds, à partir duquel les acheteurs éligibles affiliés à l'organisation effectuant l'achat peuvent acquérir les technologies cloud et les services associés répondant à leurs besoins. Véritable vecteur des contrats de cloud, les accords-cadres permettent d'acheter efficacement des services de cloud. Les organisations effectuant l'achat et les entités d'utilisateurs finaux ont ainsi accès à un éventail complet de services de cloud et bénéficient de tous les avantages du cloud : adaptabilité, importantes économies à grande échelle, évolutivité pour bénéficier d'une disponibilité supérieure à un prix inférieur, étendue des fonctionnalités, rythme d'innovation et capacité à évoluer dans de nouveaux secteurs géographiques.

Notez que **ce document se concentre sur l'achat de technologies cloud d'infrastructure en tant que service (IaaS) et de plateforme en tant que service (PaaS), fournies par un *CISP (Cloud Infrastructure Service Provider, Fournisseur de service d'infrastructure de cloud)*.** Ces technologies cloud peuvent être achetées directement

auprès d'un CISP ou via un revendeur CISP. *D'autres considérations d'AO seraient requises pour les distributeurs de services marketplace de cloud (PaaS et SaaS) et les services de consulting relatifs au cloud.*

Veuillez noter également que ce document ne couvre pas tous les aspects de la création d'un cadre d'approvisionnement de cloud de bout en bout. De nombreux autres documents du secteur et d'analystes couvrent des sujets tels que les bonnes pratiques d'approvisionnement cloud, la budgétisation pour le cloud, la gouvernance du cloud, etc. Nous vous conseillons vivement de prendre en compte ces conseils et documents lors du développement d'une stratégie d'approvisionnement de cloud globale.

Le **Tableau 1** ci-dessous offre un aperçu du manuel d'AO de services de cloud et de la localisation d'un exemple d'AO pour chaque composant d'un AO de services de cloud.

Tableau 1 : Sommaire des sections du manuel d'AO de services de cloud

Section	Vue d'ensemble et exemple de texte d'AO
1.0 Vue d'ensemble d'un accord-cadre de cloud	Aperçu général du modèle d'accord-cadre de cloud (LOT, comment être compétitif et contrat)
2.0 Vue d'ensemble de l'AO de services de cloud	Exemple générique de texte d'AO couvrant les sections ci-dessous, et commentaire expliquant la logique de la structure d'AO de services de cloud et le texte utilisé.
2.1 Mise en place de l'AO de services de cloud	2.1.1 Introduction et objectifs stratégiques 2.1.2 Calendrier de réponse à l'AO 2.1.3 Définitions 2.1.4 Description détaillée du modèle d'achat et de la concurrence dans l'accord-cadre 2.1.5 Exigences minimales pour le soumissionnaire - Administratif
2.2 Technique	2.2.1 Exigences minimales 2.2.2 Comparaison entre les fournisseurs 2.2.3 Établissement de contrat
2.3 Sécurité	2.3.1 Exigences minimales 2.3.2. Comparaison entre les fournisseurs 2.3.3 Établissement de contrat
2.4 Tarification	2.4.1 Exigences minimales 2.4.2 Comparaison entre les fournisseurs
2.5 Configuration de l'exécution du contrat/Conditions générales	2.5.1 Conditions générales 2.5.2 Comment faire un choix parmi les bénéficiaires par projet 2.5.3 Intégration et départ
3.0 Meilleures pratiques/Leçons apprises	3.1 Gouvernance du cloud 3.2 Budgétisation pour le cloud 3.3 Comprendre le modèle commercial du partenaire 3.4 Courtiers de cloud 3.5 Approvisionnement pré-AO/étude de marché

Section	Vue d'ensemble et exemple de texte d'AO
Annexe A - Exigences techniques pour la comparaison entre les soumissionnaires	Liste d'exigences technologiques cloud génériques pour contrats exécutoires ou mini compétitions
Annexe B - Démonstration	Exemple de script pour le produit de technologie cloud expliquant la notation (démos cloud dans le cadre d'un contrat exécutoire ou d'une mini compétition)

1.0 Vue d'ensemble d'un accord-cadre de cloud

Un accord-cadre de cloud bien conçu peut permettre d'acheter des services de cloud de manière avantageuse pour les organisations du secteur public et les fournisseurs de cloud participants. Les avantages d'un accord-cadre de cloud bien conçu comprennent :

- Nature coopérative :
    - L'association de plusieurs organisations afin de passer des commandes pour des exigences similaires offre commodité, efficacité, coûts réduits et simplification du processus de commande. Elle constitue un bon moyen de regrouper la demande de plusieurs organisations du secteur public pour les technologies cloud communes et les services de cloud associés, comme les solutions marketplace et le consulting.
- Gamme complète de services de cloud :
    - Un accord-cadre de Cloud peut inclure tous les services de consulting/professionnels/managés nécessaires pour soutenir et exécuter entièrement la migration vers le cloud et les applications associées dans le cloud, en plus des technologies cloud fournies par le CISP et des solutions marketplace.
    - Ces technologies cloud peuvent être achetées directement auprès d'un CISP ou via un revendeur désigné.
- Gouvernance de contrat :
    - Un accord-cadre de Cloud fédère des acheteurs appartenant à diverses organisations autour d'un ensemble commun de conditions générales et d'un contrat principal unique, plutôt que d'avoir des contrats distincts pour chaque organisation.
    - Il profite également aux fournisseurs, car il offre une procédure d'acquisition, des conditions générales et un mécanisme de commande standard, plutôt que des processus propres à chaque organisation du secteur public.
    - Il offre de la flexibilité. La création, l'approbation et l'exécution d'un contrat cloud efficace dans le respect des politiques/réglementations gouvernementales existantes nécessitent des essais et la capacité à s'adapter rapidement. Il est plus intéressant de créer un accord-cadre favorisant la collaboration entre le secteur public et les fournisseurs de cloud en vue de l'amélioration du contrat, de manière contractuelle, mécanique et efficace. Un contrat sur plusieurs années qui n'est pas adapté et ne peut pas être ajusté aboutit à une mauvaise expérience pour les utilisateurs finaux du secteur public, les organisations d'approvisionnement et les fournisseurs de cloud.

- Choix :
    - Un accord-cadre de Cloud permet aux acheteurs de faire leur choix parmi plusieurs CISP qualifiés et place la barre haut pour tous les services de cloud et services associés, comme un marché PaaS/SaaS de cloud et le consulting relatif au cloud.
    - Il permet de contrôler le nombre de fournisseurs sur un cadre donné, veillant ainsi à ce que le standard de chaque entité bénéficiaire soit correctement examiné.

Un accord-cadre pour acheter des services de cloud est plus efficace lorsqu'il inclut des technologies IaaS/PaaS fournies par des CISP, ainsi qu'un marché PaaS/SaaS, et les services de consulting auxquels les utilisateurs finaux du serveur public peuvent accéder, si nécessaire, pour obtenir de l'aide dans la planification, la transition, l'utilisation et l'entretien d'une application qui s'exécute dans le cloud. Par conséquent, nous recommandons de diviser un AO de services de cloud visant à mettre en place un accord-cadre de cloud en trois lots, comme indiqué ci-dessous :

- LOT 1 : TECHNOLOGIES CLOUD
  Technologies cloud achetées directement auprès d'un CISP ou via un revendeur CISP désigné.

- LOT 2 : MARKETPLACE
  Accès à une marketplace de services PaaS et SaaS.

- LOT 3 : CONSULTATING RELATIF AU CLOUD
  Services de consulting liés au cloud (formation, services professionnels, services managés, etc.) et support technique.

*Comme indiqué précédemment, ce document se concentre sur l'achat de technologies cloud IaaS et PaaS (**LOT 1**) telles que fournies par un CISP (achetées directement auprès d'un CISP ou d'un revendeur CISP). Des exigences de qualification de fournisseur distinctes seraient nécessaires pour les fournisseurs des LOTS 2 et 3 d'un AO de services de cloud.*

L'image 1 ci-dessous présente une vue générale de la façon dont un AO de services de cloud bien structuré, divisé entre ces trois lots, peut mener à un accord-cadre de cloud fournissant aux entités du secteur public de l'adaptabilité (à la fois technique et contractuelle), de la visibilité et un contrôle des dépenses et de l'utilisation cloud, ainsi que la possibilité de bénéficier de tous les services cloud nécessaires à la création et au maintien des solutions dont elles ont besoin.

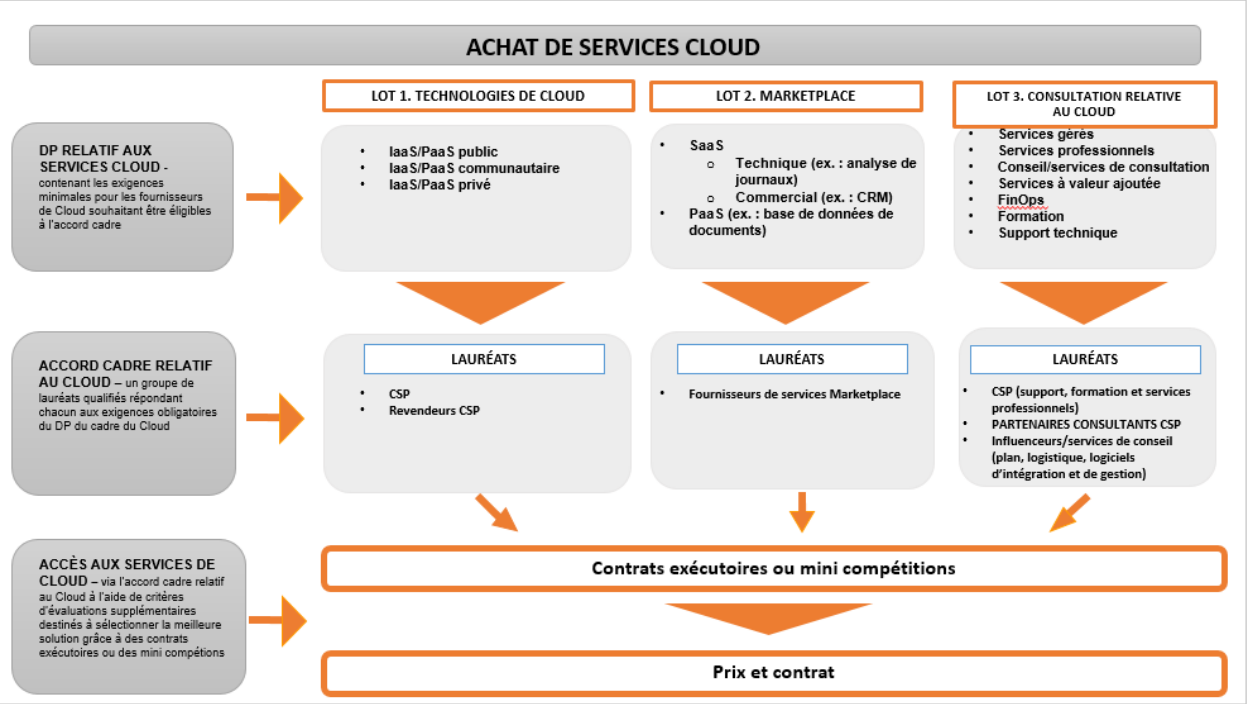

Image 1 : un AO de services de cloud réussi se divise en trois lots. Chaque lot contient des catégories ou « types d'offres » sous le lot correspondant, visant à assurer l'adéquation technique et contractuelle pour répondre aux exigences de l'utilisateur final lors de l'achat de l'accord-cadre de cloud.

Notez que :

- Chaque lot contient plusieurs attributions.
- Le LOT 3 peut être attribué via un autre AO ou via un contrat existant pour des services de consulting.

Catégories du LOT 1

Les accords-cadres de cloud réussis demandent aux CISP de décrire le modèle de cloud qu'ils proposent, divisé en catégories sous chaque lot. Nous recommandons l'utilisation du standard du secteur pour le cloud computing (les caractéristiques cloud essentielles du National Institute of Standards and Technology (NIST)) en ce qui concerne les définitions de cloud **public**, du cloud **communautaire** et du cloud **privé**. Une telle structure d'accord-cadre de cloud permet à l'agence effectuant l'achat et aux organismes publics utilisant le cadre de faire leur choix parmi différents modèles de cloud adaptés à leurs besoins.

Consultez la *Section 2.1.3 Définitions* pour accéder à la définition du NIST de chaque modèle de cloud sous le LOT 1 (IaaS/PaaS public, IaaS/PaaS communautaire et IaaS/PaaS privé).

Comment être compétitif : contrats exécutoires ou mini compétitions ?

Les critères de qualification pour un AO de services de cloud doivent couvrir des éléments essentiels et des standards minimaux, et ne doivent pas inclure des standards « qu'il serait bon d'avoir ». En cas d'ajout de

standards supplémentaires dépassant la référence des fournisseurs qualifiés pour le cadre, certains fournisseurs peuvent se retrouver dans l'incapacité de faire une offre. Cette situation peut mener à une limitation du choix pour les acheteurs.

Suite à l'AO et à la mise en place de l'accord-cadre de cloud, les organismes du secteur public bénéficiaires peuvent commander ou annuler les services de cloud lorsqu'ils en ont besoin. La conclusion d'un contrat exécutoire en vertu d'un accord-cadre permet aux acheteurs d'affiner leurs exigences en ajoutant des spécifications fonctionnelles pour une annulation, tout en conservant les avantages offerts par l'accord-cadre.

Si nécessaire, une mini compétition peut être organisée afin d'identifier le meilleur fournisseur pour une application ou un projet en particulier. Au cours d'une mini compétition, un client ouvre la compétition en vertu de l'accord-cadre et invite tous les fournisseurs d'un lot à répondre à un ensemble d'exigences. Le client invitera tous les fournisseurs aptes dans le lot à faire une offre, ce qui souligne l'importance des exigences minimales pour les bénéficiaires d'un AO de services de cloud : elles garantissent un grand nombre d'options pour chaque lot.

*Notez qu'il est important de disposer d'**ensembles distincts de conditions générales** de contrat pour chacun des lots répertoriés dans l'image 1 ci-dessus. Une approche unique pour les contrats de tous les lots créerait des problèmes en termes de compatibilité et de faisabilité technique.*

2.0 Vue d'ensemble de l'AO de services de cloud

Cette section décrit le modèle et la portée de l'AO de services de cloud, comprenant les objectifs stratégiques, les participants, les définitions, le calendrier et les exigences administratives minimales. Notez à nouveau que ce manuel se concentre sur le LOT 1 : TECHNOLOGIES CLOUD.

2.1 Mise en place de l'AO de services de cloud

Nous recommandons vivement aux entités du secteur public de clarifier leurs objectifs et exigences de haut niveau dans l'Introduction d'un AO de services de cloud.

2.1.1 Introduction et objectifs stratégiques

Pour plus de clarté en termes d'objectifs stratégiques, une bonne pratique consiste à exposer dans l'introduction d'un AO de services de cloud : **(1)** les objectifs et avantages commerciaux que l'organisation souhaite atteindre en utilisant le cloud ; **(2)** la structure de l'accord-cadre : qui achète, qui exploite, qui définit le budget, etc. ; **(3)** une explication claire du modèle de responsabilité partagée entre le secteur public et les fournisseurs de cloud, essentielle à la réussite de l'achat et de l'utilisation du cloud ; et **(4)** le type de relation créée entre les fournisseurs de service de cloud (CISP), les distributeurs des services de marché, les partenaires de consulting, les agences d'approvisionnement gouvernementales, et les utilisateurs finaux du gouvernement. L'articulation de ces quatre points aide les organisations à bâtir un AO qui répond pour le mieux à leurs besoins, en plus de veiller à ce que les clients comme les fournisseurs comprennent bien les objectifs de l'AO.

Un AO de cloud est volontairement différent des AO informatiques traditionnels. La technologie cloud ne remplace pas à l'identique les méthodes de calcul traditionnelles. Elle introduit une toute nouvelle façon d'utiliser la technologie. Les AO de services de cloud bien conçus peuvent aider les entités du secteur public à évoluer rapidement pour tirer parti du cloud.

Parmi tous les aspects d'achat de cloud que nous citons en tant que bonnes pratiques, le meilleur point de départ est probablement une bonne compréhension du modèle de responsabilité partagée. Le modèle de responsabilité partagée[1] est surtout utilisé pour ce qui a trait à la sécurité et à la conformité dans le cloud, mais cette définition des responsabilités s'applique à tous les aspects des technologies cloud. Un AO de services de cloud doit définir clairement ce qui fait partie des attributions d'un CISP dans un environnement cloud et ce qui relève de la responsabilité du client. Par exemple, un CISP fournit des fonctionnalités de supervision des ressources et applications qui s'exécutent dans le cloud, ***mais*** la responsabilité d'utiliser ces fonctionnalités fournies par le CISP revient au client. En effet, un CISP agissant à grande échelle n'est pas censé faire cela pour des millions de clients.

De plus, les clients cloud doivent comprendre comment le réseau de partenaires d'un CISP permet aux clients d'utiliser le cloud et de gérer leurs responsabilités. Par exemple, un fournisseur de service managé (MSP, Managed Service Provider) cloud peut aider un client à configurer et utiliser des fonctionnalités de supervision fournies par un CISP, afin de répondre à leurs exigences uniques de conformité et d'audit.

[1] Consultez la Section 5 du Code de conduite pour les fournisseurs de services d'infrastructure de cloud : https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

En d'autres termes, les responsabilités au sein du modèle de cloud sont les suivantes :

Un CISP fournit une technologie cloud

Un client utilise la technologie cloud

Les entreprises de consulting (le cas échéant) aident un client à accéder à la technologie cloud et à l'utiliser

Les « entreprises de consulting » *sont des entreprises de consulting et de services managés/professionnels qui aident les clients à concevoir, bâtir, créer, procéder à la migration et gérer leurs charges de travail et applications dans le cloud. Ces entreprises comprennent les intégrateurs système, les entreprises consulting stratégique, les agences, les fournisseurs de services gérés et les revendeurs à valeur ajoutée.*

Considérez l'achat de services de cloud comme l'achat dans un magasin de bricolage. Les magasins de bricolage proposent un vaste ensemble de matériaux et d'outils pour créer ce dont vous avez besoin. Vous pouvez fabriquer une armoire ou une piscine, ou même toute une maison, si vous le souhaitez. Lorsque vous achetez des matériaux et des outils, l'équipe du magasin de bricolage peut vous donner des conseils et vous faire profiter de son savoir-faire, mais elle ne peut pas venir chez vous et créer quelque chose pour vous. Plusieurs options s'offrent alors à vous :

1. Acheter les matériaux et outils vous-même et fabriquer quelque chose.
2. Acheter les matériaux et outils vous-même et engager quelqu'un qui fabriquera et/ou utilisera quelque chose pour vous.
3. Engager quelqu'un qui fabriquera/utilisera quelque chose pour vous, et lui demander de fournir les matériaux et outils nécessaires dans le cadre de son offre globale.

Si une organisation possède les compétences internes pour créer et gérer elle-même son environnement cloud et ses solutions, elle n'a besoin que de l'accès aux technologies et outils cloud standardisés du CISP (directement auprès d'un CISP ou via un revendeur CISP ; voir **LOT 1).** Les logiciels SaaS et PaaS nécessaires doivent être disponibles sur une marketplace cloud (**LOT 2**). Si une aide supplémentaire en consulting, migration, implémentation et/ou gestion est nécessaire, le réseau de partenaires d'un CISP entre en jeu (**LOT 3**).

Exemple de texte d'AO : introduction et objectifs stratégiques

Le cloud computing offre aux organisations du secteur public un accès rapide à une large gamme de ressources informatiques flexibles et économiques, avec paiement en fonction de l'utilisation réelle. Les organisations peuvent fournir le type et la taille des ressources adaptés dont ils ont besoin pour alimenter leurs nouvelles idées ou exploiter leurs services informatiques. Les investissements importants dans le matériel et/ou les contrats de licence logicielle à long terme ne sont plus nécessaires.

*L'**<ORGANISATION>** formule l'exigence de pouvoir accéder à ces types de technologies cloud commercialement disponibles afin de pouvoir répondre à ses besoins commerciaux dans un large éventail d'organisations affiliées.*

Le principal objectif du présent AO est d'attribuer un ***<ACCORD-CADRE>*** *parallèle non exclusif avec jusqu'à* ***<x>*** *fournisseurs représentant différentes technologies cloud, ainsi que des services liés au cloud.*

1. ***LOT 1****. Fournisseurs de services cloud (CISP) ou revendeurs CISP pour l'achat de technologies cloud*
2. ***LOT 2.*** *Fournisseurs de services de marketplace.*
3. ***LOT 3.*** *Fournisseurs de services de consulting pour apporter leur expertise supplémentaire dans la migration vers ces offres CISP et leur utilisation*

Concernant le ***LOT 1****, les organisations offrantes (CISP ou revendeurs CISP) doivent expliquer comment leur offre répond à ces objectifs :*

- ***Adaptabilité :*** *mettre les ressources informatiques à la disposition des utilisateurs finaux en quelques minutes au lieu des délais traditionnels de plusieurs semaines ou mois.*
- ***Innovation :*** *bénéficier d'un accès instantané aux technologies les plus récentes et innovantes sur le marché.*
- ***Coût :*** *remplacer les dépenses de capital par des dépenses variables (par ex. CapEx contre OpEx). Ne payer que ce qui est consommé.*
- ***Budgétisation :*** *consulter les informations de facturation et d'utilisation au niveau granulaire etau niveau global, en visualisant les schémas de dépenses au fil du temps, en plus de prévoir les dépenses futures.*
- ***Souplesse :*** *bénéficier de coûts variables réduits grâce à des économies d'échelle supérieures fournies par le cloud.*
- ***Capacité :*** *éliminer les hypothèses en termes de besoins de capacité d'infrastructure.*
- ***Cesser de s'appuyer sur les Datacenters :*** *se concentrer sur l'activité de nos citoyens et non sur les tâches fastidieuses et à faible valeur ajoutée consistant à racker, à stocker et à alimenter des serveurs.*
- ***Sécurité :*** *formaliser la conception de compte avec une visibilité et une auditabilité supérieures des ressources, et éliminer le coût de protection des sites et du matériel physique.*
- ***Responsabilité partagée :*** *soulager la charge opérationnelle car le CISP exploite, gère et contrôle les composants depuis le système d'exploitation hôte jusqu'à la sécurité physique des installations dans lesquelles les services sont exploités, en passant par la couche de virtualisation.*
- ***Automatisation :*** *intégrer l'automatisation dans l'architecture de cloud pour améliorer la capacité à évoluer en toute sécurité, de manière plus rapide et économique.*
- ***Gouvernance cloud :*** *(1) commencer par un inventaire complet de toutes les ressources informatiques ; (2) gérer toutes ces ressources de manière centralisée ; et (3) créer des alertes sur l'utilisation/la facturation/la sécurité/etc., avec des fonctionnalités pour le suivi des ressources, la gestion des stocks, la gestion des modifications, la gestion et l'analyse des journaux, ainsi que la visibilité globale et la gouvernance cloud.*
- ***Contrôle :*** *bénéficier d'une visibilité complète sur la consommation des services informatiques et sur leur adaptation en termes de sécurité, de fiabilité, de performances et de coûts.*
- ***Réversibilité :*** *outils et services de portabilité pour aider à migrer vers et depuis l'infrastructure du CISP, en minimisant la dépendance au fournisseur et dans le respect du ou des codes de conduite du secteur.*

- ***Protection des données :*** *capacité à démontrer la conformité au Règlement général sur la protection des données (RGPD), via un code de conduite de secteur dédié pour les services d'infrastructure de cloud : le Code de conduite de protection des données du CISPE.*
- ***Transparence :*** *les clients doivent être autorisés à connaître la localisation des infrastructures utilisées pour traiter et stocker leurs données (quartier).*

2.1.2 Calendrier de réponse à l'AO

La bonne pratique consiste à fournir aux soumissionnaires un calendrier de l'activité d'offre prévue lors de la création d'un accord-cadre de cloud et de l'AO de services de cloud associé. Il est préférable de s'engager fortement avec le secteur, car toutes les parties pourront ainsi clairement comprendre les exigences de l'AO et la manière dont tous les services de fournisseurs s'adaptent au modèle de services de cloud.

Notez que le calendrier de l'AO est soumis aux lois locales et aux obligations légales. La liste fournie ci-dessous est conçue pour être un guide de bonnes pratiques, par opposition à une liste normative d'activités et de délais.

Exemple de texte d'AO : délai de réponse

Consultez le calendrier ci-dessous pour l'AO de services de cloud :

Calendrier de l'AO de services de cloud
• *Publication de la demande d'informations (RFI, Request for Information) :* • *Réponse à l'AO :* • *Publication de la version préliminaire de l'appel d'offres (AO) :* • *Date d'échéance de la version préliminaire de la réponse à l'AO :* • *Phase de consultation du secteur : <délais>* • *Publication AO préqualification :* • *Réponse AO préqualification :* • *Publication AO :* • *Date d'échéance des questions du 1er tour :* • *Réponses du 1er tour :* • *Date d'échéance des questions du 2e tour :* • *Réponses du 2e tour :* • *Date d'échéance de la réponse à l'AO :* • *Période de clarification de l'offre :* • *Période de négociation* • *Date d'intention d'attribution :* • *Attribution de contrat :* • *Durée du contrat (options de prolongation) :*

Notez que le calendrier de l'AO est soumis aux lois locales et aux obligations légales. La liste fournie ci-dessous est conçue pour être un guide de bonnes pratiques, par opposition à une liste normative d'activités et de délais.

2.1.3 Définitions

Un AO de services de cloud doit inclure une liste détaillée de définitions. Cette liste inclut les rôles du fournisseur (par ex., fournisseur de service de cloud, revendeur cloud, partenaire fournisseur), les concepts technologiques généraux (serveur / instance, stockage, IaaS/PaaS, SaaS) et les autres éléments essentiels de l'accord. Vous trouverez ci-dessous un exemple de liste de définitions :

Exemple de texte d'AO : définitions

Les définitions ci-dessous sont les définitions du cloud computing du National Institute of Standards and Technology (NIST).[2]

- ***Infrastructure en tant que service (IaaS).*** *La fonctionnalité fournie au consommateur est d'apporter des capacités de mise en service, de traitement, de stockage, de réseaux et d'autres ressources de calcul fondamentales permettant au consommateur de déployer et d'exécuter des logiciels de son choix, ce qui peut inclure des systèmes d'exploitation et des applications. Le consommateur ne s'occupe pas de la gestion et du contrôle de l'infrastructure de cloud sous-jacente, mais exerce un contrôle sur les systèmes d'exploitation, le stockage et les applications déployées, et éventuellement un contrôle limité sur certains composants de mise en réseau (par ex., pare-feu hôte).*

- ***Plateforme en tant que service (PaaS).*** *Le client bénéficie de la capacité à déployer sur l'infrastructure de cloud des applications créées ou acquises par le consommateur, créées à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur. Le consommateur ne s'occupe pas de la gestion et du contrôle de l'infrastructure de cloud sous-jacente, comprenant le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais contrôle les applications déployées et éventuellement les paramètres de configuration pour l'environnement d'hébergement d'application.*

- ***Logiciel en tant que service (SaaS).*** *Le client a la capacité d'utiliser les applications du fournisseur s'exécutant sur une infrastructure de cloud. Les applications sont accessibles à partir de différents appareils de client grâce à une interface client léger, comme un navigateur Web (par ex., courriel accessible sur le Web) ou une interface de programme. Le consommateur ne s'occupe pas de la gestion et du contrôle de l'infrastructure de cloud sous-jacente comprenant le réseau, les serveurs, les systèmes d'exploitation, le stockage, ou même les fonctionnalités d'application individuelles, à l'exception peut-être des paramètres limités de configuration d'application spécifiques à l'utilisateur.*

- ***Cloud public.*** *L'infrastructure de cloud est mise à disposition pour une utilisation ouverte par le grand public. Elle peut être détenue, gérée et exploitée par une organisation commerciale, académique ou gouvernementale, ou plusieurs organisations de ces types. Elle existe sur le site du fournisseur de cloud.*

- ***Cloud communautaire.*** *L'infrastructure de cloud est mise à disposition pour une utilisation exclusive par une communauté spécifique de consommateurs provenant d'organisations partageant les mêmes inquiétudes (par ex., mission, exigences de sécurité, politique et considérations en matière de conformité). Elle peut être détenue, gérée et exploitée par une ou plusieurs organisations de la communauté, un tiers ou plusieurs organisations et tiers, et peut exister sur site ou hors site.*

- ***Cloud hybride.*** *L'infrastructure de cloud est composée de deux infrastructures de cloud distinctes ou plus (privé, communautaire, ou public) qui restent des entités uniques, mais sont associées par une technologie normalisée ou propriétaire qui permet la portabilité des données et des applications (par ex., « cloud bursting » pour l'équilibrage de charge entre les clouds).*

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- ***Cloud privé.*** *L'infrastructure de cloud est mise à disposition pour un usage exclusif par une seule organisation comprenant plusieurs consommateurs (par ex., unités commerciales). Elle peut être détenue, gérée et exploitée par l'organisation, un tiers ou plusieurs organisations et tiers, et peut exister sur site ou hors site.*

2.1.4 Description détaillée du modèle d'achat et de la concurrence dans l'accord-cadre

Comme indiqué ci-dessus, les organisations du secteur public doivent identifier le modèle de fonctionnement d'un accord-cadre en tant que mécanisme d'achat pour les technologies cloud, et les services associés de mise en œuvre et de gestion. Ce point doit être clarifié dans l'AO de services de cloud, afin que les fournisseurs de technologie cloud, les organisations de services de consulting, les distributeurs marketplace et les entités acheteuses comprennent leurs rôles respectifs.

Concernant la portée de l'accord-cadre, et conformément aux contrats exécutoires ou mini compétitions, les organisations doivent tenir compte des points suivants :

- Qui sera responsable de l'intégration et des services managés impliquant l'utilisation des technologies cloud en vertu du contrat.
- Est-il nécessaire qu'un revendeur/partenaire CISP fournisse des services à valeur ajoutée, autres que le maintien d'une relation contractuelle avec le CISP, fournissant des services de facturation consolidés et un accès direct et en temps voulu aux données d'utilisation et de facturation associées à l'utilisation des services de fournisseur de cloud ?
- Est-il nécessaire de faire appel à un revendeur à valeur ajoutée offrant des services complets, à un intégrateur système ou à un fournisseur de services managés, ou à toute forme de services de main-d'œuvre informatiques ?

Il est important de noter qu'un CISP n'est pas un intégrateur de système (SI, Systems Integrator) ni un fournisseur de service managé (MSP, Managed Service Provider). De nombreux clients du secteur public auront besoin d'un CISP pour leur IaaS/PaaS, et délègueront le consulting et la planification, la migration et la gestion informatiques à un SI ou MSP. L'image 2 ci-dessous décrit les rôles et responsabilités dans un modèle de services de cloud.

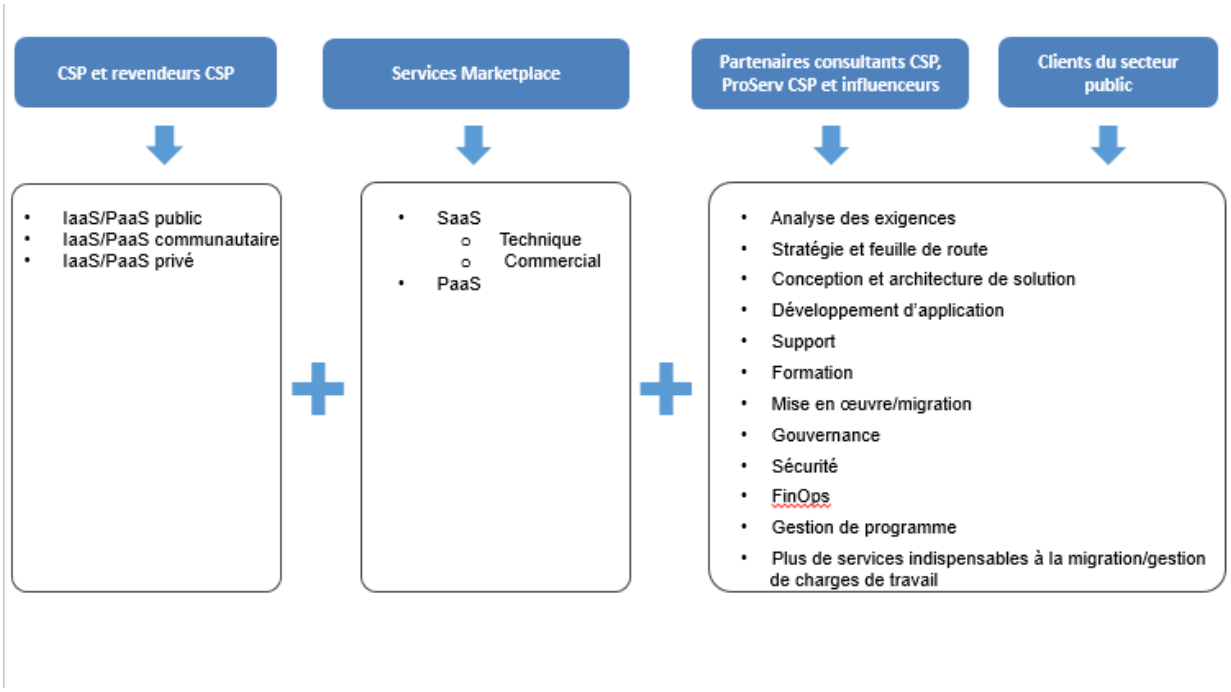

Image 2 : un AO de services de cloud doit fournir aux utilisateurs finaux un menu de tous les services de cloud dont ils ont besoin. Les clients du secteur public auront besoin d'un CISP pour les technologies cloud, d'une marketplace pour les produits PaaS et SaaS si besoin, puis le client pourra déterminer l'importance du rôle qu'il veut jouer dans l'apport de services de cloud et la part qu'il souhaite déléguer à une entreprise de consultation/un intégrateur systèmes/un fournisseur de services managés/etc.

L'exemple de texte ci-dessous s'appuie sur les rôles et responsabilités indiqués dans l'image 2 ci-dessus. Un accord-cadre de cloud et l'AO de services de cloud associé, doivent veiller à ce que les acheteurs puissent évaluer de manière adéquate les offres de chaque fournisseur, ce qui leur permettra ensuite de faire leur choix parmi les services requis pour l'application/le projet. La meilleure façon de procéder consiste à séparer les services en lots, comme indiqué précédemment, et à déterminer clairement comment sont menés les contrats exécutoires et les mini compétitions en vertu de l'accord-cadre.

Exemple de texte d'AO : modèle d'achat

Ce contrat servira de vecteur d'achat pour le ***Cadre****. Cet accord-cadre de cloud comprendra plusieurs* ***lots*** *tels que définis par l'<****ORGANISATION****>, pour les technologies cloud et les services/produits de marketplace associés, les services de consulting, les services professionnels/l'intégration système/les services managés/les services de migration professionnelle, la formation et le support, tels que définis par l'<****ORGANISATION****>, et sera utilisé par plusieurs acheteurs éligibles affiliés à l'<****ORGANISATION****>. Cela simplifiera le processus d'acquisition tout en optimisant les économies d'échelle.*

Une fois établi, cet accord-cadre permet à une organisation d'acheter les technologies cloud spécifiques et les services liés au cloud souhaités au moment de leur choix, par opposition à l'achat via des approvisionnements distincts. Ce type d'approche réduit les exigences administratives et diminue fortement la complexité et la durée du cycle d'approvisionnement.

La durée de l'accord-cadre sera au maximum de ***<X>*** *années, renouvellements inclus. La durée maximale d'un contrat exécutoire de cadre est généralement de* ***<x>*** *mois ; cette durée peut être prolongée de* ***<x>*** *mois, puis à nouveau de*

*<x> mois, avec les approbations internes appropriées, si nécessaire, pour la prolongation du contrat. Ce point sera spécifié dans chaque **Contrat exécutoire** spécifique.*

*Le CADRE se divise en **3 (trois) lots**.*

1. *LOT 1 : TECHNOLOGIES CLOUD - portée globale des technologies du fournisseur de cloud (directement par le CISP, le revendeur, ou le revendeur avec des services/support à valeur ajoutée) :*
    i. ***Services IaaS et PaaS :** menu de technologies cloud, par ex. serveur / instance, stockage, mise en réseau, base de données, analytique, services d'application, déploiement, gestion, développeur, Internet des objets (IoT), etc.). Comprend des solutions de technologie cloud en package comme DR/COOP, Archive, Big Data et analytique, DevOps, etc.*
2. *LOT 2 : MARKETPLACE – portée globale des services/produits PaaS et SaaS comme la comptabilité, la gestion de la relation client, la conception, les RH, les systèmes d'information géographique et la cartographie, le calcul haute performance, la veille économique, la gestion de contenu, l'analyse de journaux, etc.*
3. *LOT 3 : CONSULTING RELATIF AU CLOUD – portée globale des services de consulting (services managés, services professionnels, services de consulting, service à valeur ajoutée, opérations financières, support technique) associés à la migration vers le cloud et à son utilisation. Ces services peuvent inclure : planification, conception, migration, gestion, support, AQ, sécurité, formation, etc.*

Les fournisseurs peuvent envoyer leurs offres à plusieurs lots.

Les fournisseurs enverront leurs offres et la tarification associée au format de leur choix.

CONCURRENCE AU SEIN DU CADRE ET ATTRIBUTION DE CONTRATS

CONTRATS EXÉCUTOIRES

Les organismes du secteur public qui font partie de l'accord-cadre peuvent commander ou annuler les services en cas de besoin. La conclusion d'un contrat exécutoire en vertu de l'accord-cadre permet aux acheteurs d'affiner leurs exigences en ajoutant des spécifications fonctionnelles pour une annulation, tout en conservant les avantages offerts par l'accord-cadre.

Les contrats attribués en vertu de l'accord-cadre pourront démontrer une piste d'audit claire en termes d'exigences pour la sélection du fournisseur dans chaque lot. Les acheteurs finaux conserveront un enregistrement des communications avec les fournisseurs, comprenant tout engagement sur le marché précoce, les questions de clarification, les courriels et les conversations en face à face.

1. RÉDACTION DES EXIGENCES DU CONTRAT EXÉCUTOIRE ET RECHERCHE D'APPROBATION INTERNE POUR L'ACHAT

Tous les acheteurs finaux éligibles à l'utilisation de l'accord-cadre créeront des équipes conjointes d'utilisateurs finaux professionnels, de spécialistes d'achat et d'experts techniques pour préparer une liste de critères indispensables et souhaités. Ces exigences permettront de déterminer quels lots sont applicables, et quel fournisseur est le mieux qualifié pour répondre aux exigences. Lors de la rédaction des exigences, les acheteurs tiendront compte des points suivants :

- *fonds disponibles pour utiliser le service ;*
- *exigences techniques et d'approvisionnement pour le projet ;*
- *critères sur lesquels se fondera le choix.*

2. RECHERCHE DE SERVICES

Les acheteurs, en vertu de l'accord-cadre, utiliseront un catalogue en ligne (un portail sur lequel seront répertoriés les bénéficiaires de l'accord-cadre qualifiés et leurs services) pour rechercher des produits/services répondant à leurs besoins identifiés. Ils choisiront les lots appropriés, puis chercheront des services.

3. EXAMEN ET ÉVALUATION DES SERVICES

Les acheteurs, en vertu de l'accord-cadre, examineront les descriptions de services pour rechercher les services qui répondent le mieux à leurs besoins en termes d'exigences et de budget. Chaque description de service comprendra :

- *Un document contenant les définitions du service ou des liens vers les définitions du service*
- *Un document contenant les conditions générales*
- *Un document de tarification (les liens vers les tarifs publics sont acceptables, en supposant qu'une liste tarifaire/un document de tarification complet est disponible sur demande)*

Le prix correspondra au coût de la configuration la plus courante du service. Cependant, la tarification dépend généralement du volume. Les acheteurs doivent donc toujours consulter le document de tarification du fournisseur ou la tarification publique, et les outils de serveur / instance du prix pour définir le prix réel des éléments achetés, ainsi que la valeur globale fournie à l'acheteur (par exemple, services pour l'optimisation et la réduction des coûts qui en résulte).

Les acheteurs, en vertu de l'accord-cadre, peuvent s'adresser aux fournisseurs pour leur demander d'expliquer leur description de service, leurs conditions générales, leur tarification ou les documents/le modèle de définition de service. Un enregistrement des conversations avec les fournisseurs sera conservé.

4. CHOIX D'UN SERVICE ET ATTRIBUTION D'UN CONTRAT

Fournisseur unique

Si un seul fournisseur répond aux exigences, il est possible de lui attribuer un contrat.

Plusieurs fournisseurs

Si plusieurs services ont été sélectionnés, l'acheteur choisira le service proposant l'offre la plus avantageuse économiquement (MEAT, Most Economically Advantageous Tender). Consultez les critères dans le tableau suivant pour l'évaluation basée sur MEAT. Les acheteurs pourront déterminer quelles caractéristiques détaillées utiliser et quelle importance leur attribuer.

Notez que l'acheteur devra peut-être :

- *étudier l'association de plusieurs fournisseurs ;*
- *obtenir des informations spécifiques concernant les remises sur volume ou d'entreprise, et les services d'optimisation de coût pour les fournisseurs.*

L'évaluation des fournisseurs doit toujours être juste et transparente. Le choix s'effectuera selon le candidat le mieux adapté, et les fournisseurs/services ne seront pas exclus sans se rapporter aux exigences du projet.

Tableau 2 : évaluation basée sur MEAT

Critères d'attribution
Coût sur toute la durée du contrat : *rapport coût-efficacité, prix et coûts de fonctionnement*
Mérite technique et adéquation fonctionnelle : *couverture, capacité du réseau et performances spécifiés dans les niveaux de service correspondants*

Gestion du service après-vente : *bureau d'assistance, documentation, fonction de gestion de compte et garantie d'approvisionnement d'une gamme de services*
Caractéristiques non fonctionnelles

MINI COMPÉTITIONS

Si nécessaire, une mini compétition peut être organisée afin d'identifier le meilleur fournisseur pour une application ou un projet en particulier. Au cours d'une mini compétition, un client ouvre la compétition en vertu de l'accord-cadre et invite tous les fournisseurs d'un lot à répondre à un ensemble d'exigences. Le client invitera tous les fournisseurs compétents du lot à faire une offre. Consultez les informations de comparaison supplémentaires dans les sections ci-dessous concernant les aspects techniques, de sécurité et de tarification/valeur.

CONTRAT

*Le service ne pourra être utilisé que lorsque l'acheteur et le fournisseur auront tous deux signé une copie du contrat. La durée maximale d'un accord-cadre est généralement de **<x>** mois ; cette durée peut être prolongée de **<x>** mois, puis à nouveau de **<x>** mois, avec les approbations internes appropriées, si nécessaire, pour la prolongation du contrat.*

Le service ne pourra être utilisé que lorsque toutes les parties concernées (l'acheteur et le fournisseur) auront signé une copie du contrat.

2.1.5 Exigences minimales pour le soumissionnaire - Administratif

Un langage clair et simple pour définir les critères de qualification de l'accord-cadre permettra d'éviter les propositions de fournisseurs de Datacenters ou de matériel traditionnels, offrant une solution classique en tant que « cloud ». Les participants à l'AO doivent démontrer comment ils respectent les exigences administratives minimales pour l'offrant indiquées ci-dessous.

Notez à nouveau que ce document se concentre sur le LOT 1 : TECHNOLOGIES CLOUD. Cependant, nous avons ajouté des informations supplémentaires sur le LOT 2 : MARKETPLACE et le LOT 3 : CONSULTING RELATIF AU CLOUD lorsqu'elles permettent de fournir un contexte général en termes d'exigences et de portée de l'AO. Par exemple, il est important d'inclure des critères de qualification minimaux pour un revendeur CISP/MSP/SI/agence de conseil/etc., et il est utile de veiller à ce qu'ils soient : (1) directement affiliés au CISP en tant que revendeur ou partenaire de distribution, (2) certifiés par un CISP pour revendre un accès direct aux offres du CISP à des entités tierces, et (3) certifiés par ce CISP concernant ses capacités et son savoir-faire.

Exemple de texte d'AO : exigences minimales pour le soumissionnaire - Administratif

Cet accord-cadre attribuera des contrats à plusieurs fournisseurs dans les catégories suivantes. Les fournisseurs doivent être un CISP commercial, un revendeur tiers d'un CISP, un distributeur de services de marketplace et/ou un fournisseur de services pour l'utilisation d'un CISP (par ex., consulting, services de migration, services managés, opérations financières, etc.). Veuillez identifier les rôles pour lesquels vous formulez une offre :

LOT 1

____ - Fournisseur direct (CISP) de service de cloud public (IaaS ET PaaS)

____ - Fournisseur direct (CISP) de service de cloud communautaire (IaaS ET PaaS)

____ - Fournisseur direct (CISP) de service de cloud privé (IaaS ET PaaS)

____ - Revendeur tiers d'un CISP (capacité à fournir un accès direct aux offres de cloud en ligne d'un CISP).

- *Identifiez l'offre du CISP pour laquelle vous pouvez revendre un accès direct : _____*
- *Fournissez une lettre du CISP confirmant que vous êtes un revendeur agréé de leurs offres : _____*

LOT 2

____ - Fournisseur direct de services de marketplace s'exécutant sur un CISP (PaaS et/ou SaaS)

____ - Distributeur de services de marketplace s'exécutant sur un CISP (PaaS et/ou SaaS)

LOT 3

____ - CISP fournissant des services professionnels

____ - Fournisseur de support technique de CISP

____- Partenaire CISP fournissant des services pour l'utilisation ou l'exploitation sur un CISP

____- Influenceur/conseiller fournissant des services pour l'utilisation ou l'exploitation sur un CISP

Indiquez le type d'offre :

- *Services managés d'applications sur un CISP (O/N) : _____*
  - *Indiquez les spécialités le cas échéant : _____*
- *Services professionnels : (O/N) : _____*
- *Consulting – Formation (O/N) : _____*
- *Consulting – Stratégie (O/N) : _____*
- *Consulting – Migration (O/N) : _____*
- *Consulting – Gouvernance cloud (O/N) : _____*
- *Consulting – Opérations financières (O/N) : _____*
- *Consulting – Autre (veuillez préciser) : _____*

Indiquez le ou les CISP pour le(s)quel(s) vous fournissez des services : _____
Fournissez une lettre du CISP confirmant votre statut de partenaire selon le modèle de CISP : _____

LOT 1 EXIGENCES ADMINISTRATIVES MINIMALES

Fournisseurs de service de cloud (CISP)
Pour être qualifié de CISP, il doit démontrer sa conformité aux exigences ci-dessous.

Critères de qualification prévus pour CISP	*Motif*
Détails de l'organisation, par ex. Nom, Structure juridique, Immatriculation/Numéro DUNS, TVA, etc.	
Taille de l'entreprise, situation économique et financière[3]	*Le client peut estimer que le CISP sera en mesure de respecter le contrat.*

[3] Notez qu'un AO de services de cloud se penche sur les informations générales de l'entreprise, ignorant le nombre d'employés dans l'entreprise et la structure interne des équipes. Avec la technologie cloud, il n'existe pas de

Motifs d'exclusion, par ex. activités criminelles/frauduleuses, etc.	
Études de cas/références client (indiquez le nombre/type d'exigences)	*Le client peut mesurer l'expérience du CISP pour fournir les services requis.*
Responsabilités sociales d'entreprise	*Il doit s'agir de versions accessibles publiquement et fournies par le CISP.*
Engagements et pratiques de durabilité disponibles publiquement.	*Le client peut voir qu'un CISP s'engage à mener son activité de la manière la plus écologique possible.*
Le CISP doit prouver son expérience dans l'innovation et l'édition de nouveaux services et fonctionnalités au cours des 5 dernières années, en particulier dans le domaine du PAAS, du machine learning et de l'analyse, du big data, des services managés et des fonctionnalités d'optimisation de l'utilisation du cloud. Les journaux des modifications publiquement accessibles ou les flux de mise à jour peuvent être utilisés pour le prouver.	*Démontre que le CISP s'efforce de fournir rapidement de nouveaux produits aux clients, puis réitère et améliore rapidement les produits. Cela permet d'offrir aux clients une infrastructure informatique de pointe sans avoir à effectuer de nouveaux investissements en capital.*

Relation entre le revendeur/partenaire et le CISP

*<ORGANISATION> exige que le principal fournisseur soit directement affilié au CISP en tant que revendeur ou partenaire de distribution, certifié par un CISP pour revendre à des entités tierces un accès direct aux offres CISP, avec des certifications fournies par les CISP indiquant leurs capacités et leurs compétences. Ainsi, <ORGANISATION> n'a pas besoin d'examiner les Conditions et Services associés à une couche supplémentaire de sous-traitance entre le fournisseur principal de l'**accord-cadre** et le CISP. Cette exigence réduit également la complexité que génèrent les couches de revendeurs supplémentaires lorsque (1) <ORGANISATION> fait preuve de diligence raisonnable afin d'assurer une attribution claire des responsabilités concernant les services à fournir, et (2) <ORGANISATION> exerce les activités quotidiennes impliquant la consommation des services de cloud.*

2.2 Technique

Un AO de services de cloud doit placer la barre haut pour les CISP en exigeant qu'ils fournissent les technologies cloud standardisées nécessaires pour qu'un client puisse élaborer sa solution personnalisée. Comme indiqué précédemment, cette différence entre les éléments standardisés et personnalisés est très importante lors de la création d'un AO de services de cloud. Les CISP proposent des services standardisés à des millions de clients. Les personnalisations dans un AO de services de cloud se concentrent donc sur des solutions et résultats supérieurs, par opposition aux méthodes, à l'infrastructure ou au matériel sous-jacents utilisés pour proposer les services de cloud permettant d'atteindre les résultats de la solution.

2.2.1 Exigences minimales

Les approvisionnements informatiques traditionnels s'appuient souvent sur les exigences commerciales développées à travers une série de sessions de travail qui documentent la façon dont l'organisation mène actuellement son activité. Répondre parfaitement à ces exigences est un processus difficile, même dans les meilleures circonstances. Si elles sont réussies, ces sessions d'exigences décrivent le processus commercial historique qui peut être vieillissant et inefficace. Si ces exigences sont ensuite intégrées à l'AO pour être

corrélation entre la garantie des performances de service et le nombre d'employés. Les AO de cloud étudient plutôt la taille globale de l'entreprise pour répondre aux exigences (échelle adéquate) et l'expérience/les performances avérées.

reproduites par le CISP, la seule solution peut être une solution personnalisée. Ce modèle est incompatible avec les approvisionnements cloud.

Les organisations du secteur public doivent comprendre leurs objectifs commerciaux et leurs besoins en matière de performances, mais ne doivent pas entrer dans les détails dans un AO, car elles imposent la conception et la fonctionnalité du système. Au lieu de cela, l'organisation doit acheter la solution la plus adéquate. Au lieu d'évaluer des propositions sur des centaines ou des milliers d'exigences normatives qui peuvent mener à un échec, les organisations doivent inclure des critères d'évaluation sur la façon dont la technologie et les services associés respecteront ou amélioreront les objectifs commerciaux - que cela réponde ou non à leurs besoins en matière de performance - et la capacité à affiner les règles commerciales grâce à la configuration.

Les AO de cloud doivent poser les bonnes questions pour bénéficier des meilleures solutions. Étant donné que les ressources physiques ne sont pas achetées dans un modèle de cloud, de nombreuses exigences d'approvisionnement de Datacenter traditionnel ne sont pas applicables. ***La réutilisation des questions liées au Datacenter mènera inévitablement aux réponses correspondantes,*** *ce qui signifie que les CISP ne pourraient pas faire d'offre, ou que cette situation pourrait mener à des contrats mal conçus qui empêcheraient les clients du secteur public de bénéficier de toutes les fonctionnalités et de tous les avantages du cloud.*

Un AO de services de cloud se concentre sur les exigences clés requises de la part d'un CISP et de services de cloud, en veillant à ce que les fournisseurs qualifiés pour le LOT 1 atteignent un niveau élevé. Les exigences ne doivent pas non plus être trop normatives, de manière à de ne pas limiter l'accès du secteur public à une large gamme de CISP qualifiés.

Exemple de texte d'AO : capacités du fournisseur de cloud

Consultez également ci-dessous les exigences administratives CISP minimales pour le LOT 1

Critères de qualification prévus pour CISP	*Motif*
Infrastructure.	
L'infrastructure CISP doit offrir au moins 2 clusters de Datacenters. Chaque cluster doit comprendre au moins 2 Datacenters connectés par une liaison au temps de latence faible afin de permettre des déploiements actif-actif hautement disponibles et la mise en œuvre de scénarios de reprise après sinistre/continuité des opérations. Les Datacenters comprenant chaque cluster doivent être physiquement isolés et indépendants les uns des autres en termes de pannes.	*Le CISP doit pouvoir offrir une infrastructure capable de créer des applications hautement disponibles, où des points de défaillance uniques peuvent être évités.*
Le CISP doit fournir des régions isolées logiquement et géographiquement. Les données client ne doivent pas être dupliquées en dehors de ces régions par le CISP.	*Les exigences de résidence de données exigent que le client contrôle entièrement la localisation de ses données.*
Le CISP doit pouvoir fournir une connectivité directe, dédiée et privée entre ses Datacenters.	*La connectivité privée est une exigence fondamentale pour pouvoir créer une infrastructure hybride et sécurisée.*

Le CISP doit fournir des mécanismes suffisants, notamment le chiffrement pour les données en transit.	*Le client peut exiger une capacité grâce à laquelle aucune donnée non chiffrée ne peut transiter.*
Certifications CISP minimales	
Le CISP doit être certifié ISO 27001	*Grâce à l'audit tiers, à la certification et à l'accréditation, les clients peuvent comparer les services (et en particulier la plateforme) en termes de qualité, de sécurité et de fiabilité. Il est essentiel de respecter un minimum de certifications.*
Le CISP doit fournir des fonctionnalités et des services qui peuvent être utilisés en conformité avec la RGDP, ce qui permet aux clients de créer des applications conformes à la RGDP.	*Le client doit pouvoir créer ou exécuter des applications en conformité avec le RGPD. L'offre de services et outils conformes au RGPD doit donc être une condition préalable.*
Le CISP doit mettre à disposition des rapports audités par des tiers, tels que les rapports SOC 1 et 2 (couvrant les localisations et services utilisés par la CE) afin d'assurer la transparence quant aux contrôles et procédures du CISP.	*Le CISP doit être transparent quant à la façon dont l'application est exploitée et gérée. Les rapports SOC sont essentiels pour assurer la confiance et la transparence.*
Caractéristiques du service	
L'infrastructure CISP doit être accessible via des interfaces de programmation (API) et une console de gestion basée sur le Web.	*L'accès en libre-service et les interfaces de programmation sont une norme requise des fournisseurs CISP pour supprimer autant que possible les intermédiaires entre l'utilisateur et le fournisseur.*
Le CISP doit proposer une base de Services comprenant : le stockage d'objet, une base de données relationnelle gérée, une base de données non relationnelle gérée, des équilibreurs de charge gérés, la supervision et la scalabilité automatique intégrée.	*La simple offre de machines virtuelles ne suffit pas à qualifier un fournisseur de cloud. Les fournisseurs de cloud doivent proposer un ensemble de services PAAS et IAAS pour accélérer et améliorer les applications du client.*
Le CISP doit permettre au Client de modifier librement son utilisation et sa configuration des services, ou de déplacer les données au sein du CISP et en dehors (offre en libre-service).	*L'accès en libre-service aux services et aux données est une exigence stricte qui permet au client d'être entièrement indépendant.*
Le CISP doit permettre une facturation de ses services en fonction de l'utilisation réelle.	*Le paiement en fonction de l'utilisation réelle permet au client d'optimiser ses applications en termes de coût, de minimiser les risques et d'exploiter le CISP pour les applications à courte durée de vie et les PoC.*
Sécurité des données et des systèmes	
Le CISP doit permettre au client de conserver le contrôle complet de ses données, lui donner la liberté de choisir où sont stockées les données (zone urbaine), et garantir qu'aucune donnée du client ne sera déplacée, sauf si le client le décide.	*Le client doit contrôler la localisation de stockage des données, la gestion de l'accès au contenu et l'accès de l'utilisateur aux services et ressources.*
Les caractéristiques du CISP doivent donner au client un contrôle complet sur ses politiques de sécurité, y compris la confidentialité, l'intégrité et la disponibilité des données et systèmes du client.	*Le client doit pouvoir définir et mettre en œuvre ses normes de sécurité dans ses applications. Il ne suffit pas de faire confiance au fournisseur pour qu'il « fasse le nécessaire » avec les données du client.*
Contrôle des coûts	

Le CISP doit disposer de mécanismes et d'outils pour permettre au client de surveiller les dépenses au fil du temps. Les outils doivent permettre la segmentation basique des coûts en fonction de l'application, du service et du compte.	
Le CISP doit proposer des outils pour alerter le client lorsqu'un seuil de coût est dépassé.	
Le CISP doit fournir des factures détaillées au client. La facture doit pouvoir être structurée de façon à diviser les coûts par application, environnement et compte.	

Le CISP doit également fournir des réponses aux questions d'exigences techniques ci-dessous.

SOLUTIONS

Le CISP doit prouver qu'il peut fournir des modèles préconçus et des solutions logicielles qui sont hébergées sur ou intégrées au CISP, pour les solutions suivantes :

- *Stockage*
- *DevOps*
- *Sécurité et conformité*
- *Big Data et analyses*
- *Applications d'entreprise*
- *Télécommunications et mise en réseau*
- *Géospatial*
- *IoT*
- *[Autre]*

Donnez un aperçu de la façon dont le CISP a été utilisé pour les applications suivantes :

- *Reprise après sinistre*
- *Développement et test*
- *Archivage*
- *Sauvegarde et restauration*
- *Big Data*
- *Calcul haute performance (HPC)*
- *Internet des objets (IoT)*
- *Sites web*
- *Informatique sans serveur*
- *DevOps*
- *Diffusion de contenu*
- *[Autre]*

2.2.2 Comparaison entre les fournisseurs

En plus des exigences minimales dans un AO de services de cloud, il est important de fournir des critères permettant de comparer les technologies CISP au cours d'une évaluation concurrentielle.

Les AO de services de cloud doivent demander de quelles fonctionnalités cloud une organisation a besoin, en comprenant qu'il appartient au client d'utiliser ces fonctionnalités pour créer sa solution. Les fonctionnalités au-delà du standard qu'un CISP peut fournir (comme des solutions préconçues via le CISP, ou des fonctionnalités d'automatisation) peuvent être utilisées pour une analyse plus approfondie des « options à valeur ajoutée » ou de la « meilleur valeur » dans un AO de services de cloud.

Le secteur public exige souvent une compétition entre les soumissionnaires à l'aide de critères d'évaluation tels que la meilleure valeur, l'offre la plus avantageuse économiquement (MEAT, Most Economically Advantageous Tender) ou le prix le plus bas. Comme les entités du secteur public prévoient cette partie d'un AO de services de cloud, il est important de créer une approche qui tient compte des fonctions uniques du cloud. Par exemple, notez que la simple comparaison des éléments entre les offres des fournisseurs de cloud (par ex., serveur / instance ou stockage) n'est pas un moyen efficace de comparer les offres. Nous vous recommandons plutôt de vous concentrer sur les solutions de niveau supérieur comme celles indiquées ci-dessus dans la section *2.2.1*. Les entités du secteur public peuvent ensuite étudier les exigences spécifiques au cloud, comme celles indiquées dans *Annexe A - Exigences techniques pour la comparaison entre les* soumissionnaires**.**

Les AO doivent indiquer les caractéristiques de cloud essentielles nécessaires pour créer sa solution cloud. Pour cela, les organisations du secteur public peuvent exploiter les caractéristiques de cloud essentielles du NIST (National Institute of Standards and Technology), en plus d'utiliser les rapports d'analystes tiers pour veiller à ce que le CISP propose l'offre de « cloud réel » la mieux adaptée, qui fonctionne à grande échelle.

Exemple de texte d'AO : comparaison entre les fournisseurs

*Le CISP doit également fournir des réponses à TOUTES les questions d'exigences techniques de l'**Annexe A**.*

Ceux qui répondent doivent posséder les caractéristiques suivantes et décrire comment leurs offres de services de cloud répondent aux cinq caractéristiques essentielles du cloud computing[4].

1) ***Libre-service à la demande :*** *celui qui répond doit offrir la possibilité de fournir de manière unilatérale les compétences de serveur / instance, comme le temps de serveur et le stockage de réseau, automatiquement selon le besoin, sans qu'une interaction humaine soit nécessaire avec chaque fournisseur de service. Il doit offrir la capacité de fournir les services de manière unilatérale (i.e. sans révision ni approbation de fournisseur) pour l'activité de commande. Expliquez comment cela fonctionne avec votre offre ou l'offre que vous représentez.*

2) ***Accès réseau omniprésent :*** *celui qui répond doit fournir plusieurs options de connectivité réseau, dont une doit être basée sur Internet. Expliquez comment cela fonctionne avec votre offre ou l'offre que vous représentez.*

3) ***Regroupement de ressources :*** *le CISP du répondant doit fournir des ressources de calcul regroupées qui servent plusieurs consommateurs à l'aide d'un modèle de locataires multiples avec différentes ressources virtuelles attribuées de manière dynamique et réattribuées en fonction de la demande des consommateurs. L'utilisateur est en mesure d'indiquer la localisation à un niveau d'abstraction supérieur (par ex., pays, région ou localisation du Datacenter). Le répondant doit prendre en charge la scalabilité de ces ressources en quelques minutes ou heures à compter de la demande d'approvisionnement. Expliquez comment cela fonctionne avec votre offre ou l'offre que vous représentez.*

4) ***Adaptabilité express :*** *le CISP du répondant doit prendre en charge les fonctionnalités d'approvisionnement et de désapprovisionnement du service (évolution à la hausse et à la baisse), pour rendre le service disponible dans les délais prescrits minimaux (maximum « x » heures) à compter de la demande d'approvisionnement. Le répondant doit prendre en charge les ajustements de facturation résultant de ces demandes d'approvisionnement quotidiennes, par heure ou par jour.*

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

5) ***Service mesuré :*** *le répondant doit offrir de la visibilité sur l'utilisation du service via un tableau de bord en ligne ou des moyens électroniques similaires.*

De plus, le CISP doit :

- *Être un leader reconnu dans l'apport de services de cloud, comme le démontre le rapport Gartner Magic Quadrant pour IaaS*[5]
- *Indiquez des rapports d'analystes tiers reconnus par le secteur qui démontrent les fonctionnalités et la fiabilité éprouvées des CISP.*

Enfin, les CISP seront comparés à l'aide des scénarios donnés dans l'Annexe B.

2.2.2.1 Accords de niveau de service (SLA)

Les CISP proposent des SLA commerciaux standardisés à des millions de clients. À la différence des modèles de Datacenter sur site, ils ne sont donc pas en mesure de proposer des SLA personnalisés. Cependant, les clients des CISP (souvent aidés de partenaires CISP) peuvent organiser leur utilisation du cloud de manière à tirer parti des SLA commerciaux des CISP, afin d'atteindre et de dépasser les exigences spécifiques du client et les SLA uniques.

Les AO de services de cloud doivent veiller à ce que les CISP proposent les fonctionnalités et les conseils nécessaires pour tirer parti de leurs services et SLA commerciaux, afin que les utilisateurs individuels finaux puissent répondre à leurs besoins de performance et de disponibilité.

Exemple de texte d'AO : accords de niveau de service

Fournissez les informations et les liens relatifs à l'approche des CISP concernant les accords de niveau de service (SLA).

L'<ORGANISATION> *maintiendra le niveau de sensibilisation aux SLA des CISP et déploiera d'importantes applications, de manière à ce qu'elles continuent de fonctionner si un SLA n'est pas respecté.*

L'<ORGANISATION> *sera responsable du maintien des SLA appropriés associés à tout l'équipement appartenant à l'****<ORGANISATION>*** *ou aux services exploités par l'****<ORGANISATION>*** *utilisés avec le CISP.*

*Le CISP doit fournir à l'****<ORGANISATION>*** *une visibilité et un suivi continus de ses performances SLA opérationnelles, ainsi que des bonnes pratiques documentées pour exploiter l'infrastructure CISP afin de créer des services performants, durables et fiables.*

2.2.3 Établissement de contrat

Les conditions générales du CISP sont conçues pour refléter le fonctionnement d'un modèle de services de cloud (les actifs physiques ne sont pas achetés et les CISP fonctionnent à grande échelle en offrant des services standardisés) ; il est donc essentiel que les conditions générales d'un CISP soient intégrées et utilisées dans toute la mesure possible. Veuillez consulter la section *2.5* ci-dessous pour plus d'informations sur les conditions générales et l'établissement de contrat.

2.2.3.1 Services nouveaux et modifiés

Les CISP fournissent des performances via un service. Contrairement aux solutions traditionnelles sur site qui requièrent des mises à niveau et des contrats de maintenance de service soumis à expiration, les

[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

fournisseurs de cloud proposent simplement le service standardisé. Pour que le modèle de cloud réalise des économies d'échelle, les mises à niveau et les modifications de l'infrastructure sous-jacente sont déployées pour tous les utilisateurs, et non de manière individuelle. Les clients choisissent ensuite les services qu'ils utilisent. Le service est plus fluide que les anciens systèmes sur site. Les fournisseurs de cloud ajoutent constamment des services nouveaux et améliorés, que les clients peuvent utiliser comme ils le souhaitent.

Si des services de CISP nouveaux ou améliorés ne peuvent pas être ajoutés après le délai de soumission d'un AO, les organisations du secteur public n'utilisent pas les nouveaux services et les fonctionnalités améliorées avant la publication de la prochaine version d'un accord-cadre. C'est pourquoi nous vous recommandons fortement d'étendre la prestation de services décrite dans l'accord-cadre. Cela permettra d'ajouter de nouveaux services CISP une fois le délai de soumission écoulé. La loi des marchés publics de l'UE peut limiter l'introduction de nouveaux services CISP sensiblement différents dans l'accord-cadre, mais les mises à jour et nouvelles versions des services qui ne sont pas considérés comme des changements importants peuvent être ajoutées sans difficulté.

Exemple de texte d'AO : services nouveaux et modifiés

*Le CISP doit fournir une solution économique qui utilise des technologies de virtualisation éprouvées et stables et des technologies de pointe constamment actualisées. L'**<ORGANISATION>** confirme et reconnaît que les technologies cloud peuvent être fournies sur une base de service partagé avec l'**<ORGANISATION>** et d'autres clients du CISP à partir d'une base de code commune et/ou d'un environnement commun, et le CISP peut, de temps à autre : modifier, ajouter ou supprimer les fonctions, fonctionnalités, performances ou autres caractéristiques des services de cloud. Si un tel ajout, modification ou suppression est effectué, les spécifications du service de cloud doivent être modifiées en conséquence.*

*La portée de ce bon de livraison comprend tous les services CISP existants, nouveaux ou améliorés **INCLUS DANS LA PORTÉE DU CADRE.** Les services de cloud fournis par le CISP et disponibles pour les clients commerciaux doivent être mis à la disposition de **<ORGANISATION>**.*

2.2.3.2 Enfermement/Réversibilité du fournisseur

La technologie cloud réduit la dépendance au fournisseur car les actifs physiques ne sont pas achetés. Les clients peuvent déplacer leurs données d'un fournisseur de cloud à un autre à tout moment.

Cependant, un certain degré de dépendance au fournisseur est inévitable lors de l'achat de services de cloud : en effet, tous les clouds ne sont pas égaux, et un CISP peut donc proposer des services et fonctionnalités qu'un autre ne peut simplement pas fournir. Cela réduit la possibilité d'utiliser ces services chez un autre fournisseur. Une approche prudente consiste à exiger que les CISP fournissent les fonctionnalités et services requis pour quitter leur cloud, avec des documents indiquant comment utiliser ces services faisant office de « stratégie de sortie » raisonnable. En effet, un CISP ne peut pas connaître la configuration unique selon laquelle un client utilise ses services standardisés, et donc fournir un plan de sortie personnalisé.

Des codes de conduite du secteur pour traiter du « Portage de données » et du « Changement de fournisseurs de cloud » sont en cours de développement afin de respecter l'Article 6 de la « réglementation sur la libre circulation des données non personnelles » de l'UE, et doivent être utilisés en tant qu'outils permettant de démontrer cette réversibilité après leur publication. Ces références seront disponibles sur le site Web du CISPE.

Exemple de texte d'AO : intégration et départ

*L'**<ORGANISATION>** cherche à recevoir des propositions fournissant une stratégie de sortie raisonnable afin d'éviter l'enfermement. L'**<ORGANISATION>** n'achète pas d'actifs physiques, et le CISP fournira la capacité à faire évoluer la pile informatique à la hausse et à la baisse. Le CISP fournira les outils et services de portabilité pour aider au transfert vers et depuis la plateforme du CISP, réduisant ainsi l'enfermement. Une documentation détaillée quant à la manière d'utiliser les outils et services de portabilité fournis par le CISP servira de plan de sortie raisonnable.*

*Le CISP ne doit pas avoir d'engagement minimal **requis** ni de contrat à long terme **requis**.*

*Les données stockées auprès d'un fournisseur de services peuvent être exportées par le client à tout moment. Le CISP permettra à l'**<ORGANISATION>** de déplacer les données selon le besoin, sur le stockage CISP et en dehors. Le CISP permettra de télécharger et de transférer les images de machines virtuelles vers un nouveau fournisseur de cloud. L'**<ORGANISATION>** peut exporter ses images de machine et les utiliser sur site ou chez un autre fournisseur (sous réserve de restrictions de licences des logiciels).*

2.3 Sécurité

Les responsabilités en matière de conformité et de sécurité incombent à la fois au CISP et aux clients du cloud. Dans ce modèle, les clients du cloud contrôlent la façon dont ils organisent et sécurisent leurs applications et données placées dans l'infrastructure. Les CISP, quant à eux, sont chargés de fournir les services sur une plateforme hautement sécurisée et contrôlée, ainsi que de proposer une vaste gamme de fonctionnalités de sécurité supplémentaires. Le niveau des responsabilités du CISP et du client dans ce modèle dépend du modèle de déploiement du cloud (IaaS/PaaS/SaaS). Les clients doivent clairement comprendre leurs responsabilités dans chaque modèle.

Il est essentiel de comprendre cette responsabilité partagée pour créer un AO de services de cloud réussi. Les organisations du secteur public doivent s'assurer de connaître les responsabilités d'un CISP, les éléments dont elles sont elles-mêmes responsables et où se situent les partenaires de consulting/éditeurs de logiciels et leurs solutions pour apporter leur aide.

2.3.1 Exigences minimales

En termes de sécurité dans le cloud, le mot-clé est **Capacité**. Les organisations du secteur public doivent être exigeantes avec les CISP et exiger qu'ils fournissent les capacités de sécurité nécessaires pour que les clients puissent endosser leurs responsabilités dans le modèle de responsabilité partagée. Comme vu dans la liste d'exigences représentatives ci-dessous, le CISP doit fournir une capacité standardisée, afin que le client puisse l'utiliser pour sécuriser son environnement cloud unique.

- ***Fournir** des pare-feu de réseau et des **capacités** de pare-feu d'application Web pour créer des réseaux privés et contrôler l'accès aux instances et aux applications.*
- ***Fournir** des **options** de connectivité qui permettent des connexions privées ou dédiées depuis votre bureau ou un environnement sur site.*
- ***Fournir** la **capacité** de mettre en œuvre une stratégie de défense approfondie et de contrecarrer des attaques DDoS.*
- ***Capacités** de chiffrement des données disponibles dans les services de stockage et de base de données.*
- ***Fournir** des **options** de gestion clés flexibles, vous permettant de demander au CISP de gérer les clés de chiffrement ou permettant au client de garder le contrôle complet des clés.*
- ***Fournir** des **API** pour permettre aux clients d'intégrer le chiffrement et la protection des données à l'un des services développés ou déployés dans un environnement CISP.*

- ***Fournir*** *des* ***outils*** *de déploiement pour gérer la création et la désactivation des ressources du CISP conformément aux standards organisationnels.*
- ***Fournir*** *des* ***outils*** *de gestion des stocks et de la configuration pour identifier les ressources du CISP, puis suivre et gérer les modifications apportées à ces dernières avec le temps.*
- ***Fournir des outils et fonctionnalités*** *qui permettent aux clients de voir exactement ce qu'il se passe dans leur environnement CISP.*
- ***Offrir*** *une grande* ***visibilité*** *sur les appels d'API, notamment de qui, de quoi et de quelle localisation émanent ces appels.*
- ***Fournir*** *des* ***options*** *d'agrégation de journaux, des enquêtes de rationalisation et des rapports de conformité.*
- *Fournir la capacité de configurer des notifications d'alerte lorsqu'un événement spécifique se produit ou que des seuils sont dépassés.*
- ***Fournir des capacités*** *pour définir, renforcer et gérer les stratégies d'accès utilisateur sur tous les services CISP.*
- ***Fournir*** *la* ***capacité*** *de définir des comptes utilisateur individuels avec des autorisations pour les ressources CISP.*
- ***Fournir*** *la* ***capacité*** *d'intégrer et d'associer des répertoires d'entreprise pour réduire les frais généraux d'administration et améliorer l'expérience de l'utilisateur final.*

Vous trouverez d'autres exigences dans *Annexe A - Exigences techniques pour la comparaison entre les* soumissionnaires**.**

Des fonctionnalités supérieures au standard minimum pour la sécurité peuvent être utilisées pour une analyse plus pertinente des « options à valeur ajoutée » ou de la « meilleure valeur » dans un AO. Il est préférable que le nombre de fonctionnalités intégrées ou automatisées en termes de sécurité soit le plus important possible. À nouveau, veuillez-vous reporter à *Annexe A - Exigences techniques pour la comparaison entre les* soumissionnaires pour connaître les exigences relatives à la comparaison des soumissionnaires.

Les organisations du secteur public doivent étudier les certifications et évaluations d'accréditation cloud pour s'assurer que les contrôles de sécurité requis du CISP sont en place. Par exemple : envisagez un CISP qui a été validé et certifié par un auditeur indépendant pour confirmer son adéquation avec la norme de certification ISO 27001. L'annexe A, domaine 14 de la norme ISO 27001 se penche sur les contrôles spécifiques auxquels un CISP adhère selon les exigences ISO autour de l'acquisition, du développement et de la maintenance du système. Il est probable que ces contrôles couvrent la majorité, voire la totalité des contrôles autour de l'acquisition, du développement et de la maintenance du système, qui seraient généralement demandés par une organisation dans un AO informatique. Il paraît donc logique qu'une organisation demande simplement à ce qu'un CISP soit certifié ISO 27001, au lieu de multiplier les efforts et de répertorier les exigences de contrôle liés à l'acquisition, au développement et à la maintenance du système dans un AO de services de cloud.

Cette approche d'exploitation des rapports de conformité tiers peut être appliquée à la plupart des contrôles de conformité et de sécurité, par ex. RGPD, ISO, SOC, etc.

Exemple de texte d'AO : sécurité

*Le CISP doit divulguer ses processus de sécurité non propriétaires et ses limitations techniques à l'****<ORGANISATION>*** *afin que le niveau de protection et de flexibilité adéquat puisse être atteint entre l'****<ORGANISATION>*** *et le fournisseur de services.*

Le CISP doit indiquer ses rôles et responsabilités en termes de sécurité et de conformité :

- *Décrire les rôles et responsabilités du CISP et de l'**<ORGANISATION>** en matière de sécurité dans l'offre proposée. Indiquer clairement la délimitation des responsabilités et préciser les services CISP pour aider l'**<ORGANISATION>** à créer et automatiser les fonctions de sécurité dans son environnement cloud.*
- *Fournir des réponses aux spécifications techniques dans l'**ANNEXE A** liées aux exigences de sécurité de l'**<ORGANISATION>**.*

PROPRIÉTÉ ET CONTRÔLE DU CONTENU DE <ORGANISATION>

*Décrire comment les capacités du CISP peuvent protéger la confidentialité des données de l'**<ORGANISATION>**. Inclure les contrôles sur place pour traiter la protection du contenu de l'**<ORGANISATION>**. Le CISP doit fournir un isolement régional fort, de sorte que les objets stockés dans une région ne quittent jamais cette région, à moins que l'<**ORGANISATION**> ne les transfère explicitement vers une autre région.*

- *L'**<ORGANISATION>** gérera l'accès à son contenu, à ses services et à ses ressources. Le CISP doit fournir un ensemble élaboré de fonctionnalités d'accès, de chiffrement et de consignation afin de permettre à l'**<ORGANISATION>** de réaliser efficacement toutes ces tâches. Le CISP n'accédera pas au contenu de l'<**ORGANISATION**> et ne l'utilisera pas à toute autre fin que dans le cadre de l'obligation légale et afin de procéder à la maintenance des services du CISP et de pouvoir les proposer à l'<**ORGANISATION**> et ses utilisateurs finaux.*
- *L'**<ORGANISATION>** choisira la (ou les) région(s) dans laquelle (lesquelles) son contenu sera stocké. Le CISP ne procèdera pas au déplacement ni à la reproduction du contenu de l'**<ORGANISATION>** en dehors de la (ou des) région(s) choisie(s), sauf en cas d'obligation légale ou de nécessité de procéder à la maintenance des services du CISP dans le but de pouvoir les proposer à l'**<ORGANISATION>** et à ses utilisateurs finaux.*
- *L'**<ORGANISATION>** choisira la manière dont son contenu est sécurisé. Le CISP doit fournir un chiffrement renforcé pour le contenu de l'**<ORGANISATION>** en transit ou inactif, et permettre à l'**<ORGANISATION>** de gérer ses propres clés de chiffrement.*
- *Le CISP doit disposer d'un programme d'assurance de sécurité faisant appel à des bonnes pratiques globales concernant la confidentialité et la protection des données afin d'aider l'**<ORGANISATION>** à s'établir et travailler au mieux dans son environnement de contrôle de la sécurité. Les éléments de protection de la sécurité et processus de contrôle doivent être validés par de nombreuses instances d'évaluation indépendantes.*

Les évaluations et les certifications d'accréditation cloud donnent aux organisations du secteur public l'assurance que les CISP ont mis en place des contrôles de sécurité physiques et logiques efficaces. Lorsque ces accréditations sont exploitées dans les AO, elles simplifient le processus d'approvisionnement et aident à éviter les processus ou flux d'approbation répétitifs et très lourds qui ne sont pas forcément nécessaires pour un environnement cloud.

Les AO de cloud doivent donner aux CISP l'occasion de prouver qu'ils respectent les accréditations et évaluations de conformité. Comme indiqué ci-dessus, il existe un chevauchement considérable dans les scénarios de risques et les pratiques de gestion des risques dans ces schémas d'accréditation. Ainsi, étant donné que les contrôles et exigences sont associés dans ces accréditations, le fait d'exiger que les CISP respectent les accréditations permet de traiter plus rapidement la conformité dans un AO, au lieu de multiplier les efforts pour lister des contrôles individuels (dont beaucoup peuvent être issus d'anciens AO concernant directement des Datacenters sur site, et ne pouvant donc pas s'appliquer au cloud computing).

REMARQUE : il est également très important de comprendre comment accéder aux rapports répertoriés ci-dessous. Par exemple, les rapports SOC 1 et SOC 2 sont généralement des documents sensibles. Comprenez les contrats nécessaires pour y accéder (par ex., accord de confidentialité – NDA) et ne

demandez pas simplement à ce que ces documents soient envoyés dans le cadre de la réponse à l'AO (ces documents peuvent être rendus publics via des actes Open Records ou une sécurité cloud similaire mettant en danger la législation).

Exemple de texte d'AO : conformité

L'utilisation de standards reconnus, dérivés des bonnes pratiques dans les opérations de service de cloud (y compris la gestion des données, leur sécurité, la confidentialité, la disponibilité, etc.), qu'ils soient opérationnels, de sécurité ou de conformité, simplifie l'approvisionnement de la technologie cloud.

L'<ORGANISATION> évaluera les offres de proposition uniques par rapport aux standards opérationnels, de sécurité et de conformité acceptés tels que définis ci-dessous et dans l'Annexe A. En s'appuyant sur la certification de conformité du fournisseur par rapport à chaque standard, l'<ORGANISATION> peut utiliser la conformité minimale par rapport au standard en tant que référence pour l'évaluation de la proposition.

Exiger que le CISP assure de façon continue le respect de la conformité selon le standard minimal sur toute la durée du contrat permet de garder la conformité du service à jour.

Le CISP faisant l'offre (directement ou via un revendeur) doit pouvoir démontrer sa capacité à respecter les attestations, rapports et certifications tiers indépendants suivants (remarque : si certains de ces rapports, attestations et certifications font l'objet de restrictions de divulgation en raison de problèmes de sécurité, l'<Organisation> travaillera avec le CISP pour obtenir un accès mutuellement convenu) :

Certifications / Attestations	*Lois, règlementations et confidentialité*	*Adéquations / Infrastructures*
☐ C5 (Allemagne)		*☐ CDSA*
☐ Code de conduite sur la protection des données CISPE (RGPD)		
☐ DIACAP	*☐ Directive sur la protection des données dans l'UE*	*☐ CIS*
☐ DoD SRG niveaux 2 et 4	*☐ Clauses types de l'UE*	*☐ Informations sur la justice pénale. Service (CJIS)*
☐ HDS (France, Santé)		
☐ FedRAMP	*☐ FERPA*	*☐ CSA*
☐ FIPS 140-2	*☐ RGPD*	*☐ Bouclier de protection des données UE – États-Unis*
☐ ISO 9001	*☐ GLBA*	*☐ Safe Harbor UE*
☐ ISO 27001	*☐ HIPAA*	*☐ FISC*
☐ ISO 27017	*☐ HITECH*	*☐ FISMA*
☐ ISO 27018	*☐ IRS 1075*	*☐ G-Cloud [Royaume-Uni]*
☐ IRAP [Australie]	*☐ ITAR*	*☐ GxP (FDA CFR 21 Partie 11)*
☐ MTCS de niveau 3 [Singapour]	*☐ PDPA – 2010 [Malaisie]*	*☐ ICREA*
☐ PCI DSS niveau 1	*☐ PDPA – 2012 [Singapour]*	*☐ IT Grundschutz [Allemagne]*

☐ *Règle SEC 17-a-4(f)*	☐ *PIPEDA [Canada]*	☐ *MARS – E*
☐ *SecNumCloud (France)*		
☐ *SOC1 / ISAE 3402*	☐ *Loi sur la protection des données [Australie]*	☐ *MITA 3.0*
☐ *SOC2 / SOC3*	☐ *Loi sur la protection des données [Nouvelle-Zélande]*	☐ *MPAA*
	☐ *Autorisation DPA - Espagne*	☐ *NIST*
	☐ *Royaume-Uni DPA - 1988*	☐ *Niveaux Uptime Institute*
	☐ *VPAT/Section 508*	☐ *Principes de sécurité du cloud - Royaume-Uni*

La liste ci-dessous a été fournie à des fins d'illustration uniquement et ne doit pas être considérée comme exhaustive pour les certifications et standards pouvant s'appliquer aux services de cloud.

2.3.2 Comparaison entre les fournisseurs

Comme pour les critères techniques dans les sections ci-dessus, en plus des exigences de sécurité minimales dans un AO de services de cloud, il est important de fournir des critères avec lesquels les services et fonctionnalités de sécurité CISP peuvent être comparés au cours d'une évaluation compétitive.

Veuillez consulter *Annexe A - Exigences techniques pour la comparaison entre les* soumissionnaires pour obtenir des exemples d'exigences de sécurité de CISP. Nous vous recommandons fortement de considérer les capacités ci-dessous comme essentielles pour les entités du secteur public évaluant les CISP :

Exemple de texte d'AO : considérations essentielles relatives à la sécurité

- *Compréhension par le CISP du modèle de responsabilité partagée, et documentation visant à aider les clients à comprendre la délimitation des responsabilités de sécurité en matière de fonctions et services CISP (par exemple, dans le contexte du RGPD)*
- *Expérience reconnue de la sécurité de l'infrastructure du CISP, avec documentation non propriétaire publiquement disponible de la sécurité et des contrôles physiques/logiques du CISP*
- *Support CISP spécifique à la sécurité du cloud*
- *Services permettant aux clients de formaliser la conception de compte, d'automatiser les contrôles de sécurité et de gouvernance du cloud, et de rationaliser les audits*
- *Capacité à créer, fournir et gérer un ensemble de ressources à la manière d'un modèle (qui comprend les modèles de sécurité de référence absolue conçus par le CISP/le partenaire du CISP)*
- *Capacité à établir des opérations de contrôle fiables et reproductibles*
- *Fonctionnalités pour des audits continus et en temps réel*
- *Capacité à créer un script technique des politiques de gouvernance cloud*
- *Capacité à créer des fonctions de protection qui ne peuvent être contournées que par les utilisateurs autorisés*
- *Capacité à mettre en œuvre de façon fiable les éléments contenus auparavant dans les stratégies, les normes et les réglementations. Ils peuvent créer parallèlement une sécurité et une conformité applicables, ce qui génère en retour un modèle de gouvernance cloud fiable et fonctionnel pour les environnements informatiques*
- *Services de protection contre les attaques par déni de service distribué (DDoS) les plus courantes et les plus fréquentes du réseau et de la couche de transport, ainsi que la possibilité d'écrire des règles personnalisées pour minimiser les attaques sophistiquées de la couche applicative*
- *Service managé de détection des menaces*

2.3.3 Établissement de contrat

Comme indiqué ci-dessus, les conditions générales du CISP sont conçues pour refléter le fonctionnement d'un modèle de services de cloud (les actifs physiques ne sont pas achetés et les CISP fonctionnent à grande échelle en offrant des services standardisés) ; il est donc essentiel que les conditions générales d'un CISP soient intégrées et utilisées dans toute la mesure possible. Veuillez consulter la section *2.5* ci-dessous pour plus d'informations sur les conditions générales et l'établissement de contrat.

En termes de sécurité, une fois de plus, nous recommandons vivement d'autoriser les CISP à mettre à jour leurs offres en permanence, ou d'autoriser les fournisseurs à ajouter des produits après le délai de soumission, s'ils sont conformes aux paramètres d'origine de l'AO. Cela témoigne du fait que les fonctionnalités et services de sécurité évoluent rapidement ; les CISP publient souvent des services axés sur la sécurité, qui sont gratuits dans de nombreux cas. Notez qu'il est important d'avoir un niveau de sécurité de référence (consultez les exigences minimales ci-dessus) afin de garantir que les modifications apportées aux offres de sécurité ne seront pas préjudiciables.

Le modèle de responsabilité partagée est naturellement au cœur de la sécurité dans un AO de services de cloud. Chaque partie doit clairement connaître ses responsabilités en matière de sécurité, les CISP, eux, doivent être tenus de documenter les responsabilités de sécurité du CISP/client pour les technologies cloud fournies par le CISP, en plus de la documentation aidant les clients à intégrer et à automatiser les bonnes pratiques de sécurité.

Un accord-cadre de cloud doit fournir la flexibilité nécessaire pour révoquer un fournisseur s'il ne respecte plus les exigences minimales de sécurité et de conformité, comme indiqué dans l'AO de services de cloud.

2.4 Tarification

Les organisations du secteur public ont besoin d'un contrat pour la technologie cloud tenant compte de la fluctuation de la demande et leur permettant de payer les services consommés. Cela doit s'accompagner de la gouvernance et de la visibilité du cloud requises en termes d'utilisation et de dépenses.

Fait important, les AO de services de cloud doivent étudier la valeur et le coût total de possession (TCO, total cost of ownership), et ne pas se contenter d'une simple comparaison des prix unitaires. Cette pratique traditionnelle, consistant à étudier le prix unitaire le plus bas, ne se traduit pas dans le modèle de cloud et ne mène généralement pas à l'offre la plus avantageuse économiquement ou au prix global le plus bas.

Pour l'évaluation de la tarification CISP, il est utile d'avoir au préalable une pré-qualification ou une « short-list » de CISP, accompagnée des ***exigences minimales liées aux tarifs****. Les CISP possédant des capacités similaires peuvent ainsi répondre aux critères de l'accord-cadre. Le processus d'évaluation pour les contrats exécutoires et les mini compétitions peut ensuite se pencher sur une sélection d'exemples typiques d'architectures de cloud et de* ***scénarios de tarification*** *correspondant à certaines charges de travail typiques du secteur public, et demander à des CISP d'en fixer le prix. Il est également recommandé de procéder à des démonstrations en direct, permettant de comparer les performances et capacités d'adaptation des services de technologies cloud fournis par les CISP. Consultez l'Annexe B pour accéder à un exemple de script de démonstration pour les technologies cloud.*

2.4.1 Exigences minimales

La section de tarification d'un AO de services de cloud comporte quatre éléments principaux :

1. **Tarification à la demande :** les clients cloud intègrent un modèle de facturation à la demande en fonction de l'utilisation, grâce auquel ils paient simplement ce qu'ils ont utilisé à la fin du mois. Cette solution est optimale pour les métriques d'utilisation et de ressources.
2. **Tarification transparente :** la tarification du CISP doit être publiquement disponible et transparente.
3. **Tarification dynamique :** inclut la flexibilité nécessaire pour permettre la fluctuation des prix du cloud d'après la tarification du marché. Cette approche tire parti de la nature dynamique et compétitive de la tarification du cloud, et soutient l'innovation et la réduction des prix.
4. **Dépenses contrôlées :** les CISP doivent proposer des outils de création de rapports, de supervision et de prévision qui permettent aux clients de (1) surveiller l'utilisation et les dépenses aux niveaux général et détaillé, (2) recevoir des alertes lorsqu'ils atteignent des seuils personnalisés d'utilisation et de dépenses, (3) estimer l'utilisation et la dépense afin de planifier les budgets de cloud à venir.

Exemple de texte d'AO : tarification

L'<ORGANISATION> demande aux CISP qui répondent d'inclure la méthode proposée et leur modèle de tarification pour fournir chacun de leurs services aux utilisateurs finaux en tant que capacité de cloud commercial.

Le CISP doit fournir :

- *Un document contenant les définitions de chaque service ou des liens vers les définitions de chaque service*
- *Un document contenant les conditions générales*
- *Un document de tarification (les liens vers les tarifs publics sont acceptables, en supposant qu'une liste tarifaire/un document de tarification complet soit disponible sur demande)*

Le prix correspondra au coût de la configuration la plus courante du service. Les CISP doivent fournir des options pour les remises sur volume et les outils de calcul du prix pour définir le prix réel des éléments achetés, ainsi que la valeur globale fournie à l'acheteur (par exemple, services pour l'optimisation et la réduction des coûts qui en résulte).

Les acheteurs, en vertu de l'accord-cadre, peuvent s'adresser aux fournisseurs pour leur demander d'expliquer leur description de service, leurs conditions générales, leur tarification ou les documents/le modèle de définition de service. Un enregistrement des conversations avec les fournisseurs sera conservé.

Exigences de tarification supplémentaires

- *Les technologies cloud doivent être fournies avec un modèle de tarification dynamique qui offre une flexibilité commerciale maximale, tout en favorisant l'évolution et le développement.*
- *Les attributs de tarification doivent inclure les éléments suivants :*
  - *La tarification est-elle fournie dans un service à la demande, de type utilitaire avec paiement à l'utilisation ? Expliquez votre modèle de tarification.*
  - *Pouvez-vous offrir d'autres remises si le client s'engage à utiliser un certain volume et/ou à acheter en lot ? Expliquez comment.*
  - *La tarification est-elle publiquement disponible et transparente ? Veuillez inclure des liens vers la tarification publiquement disponible.*
  - *La tarification est-elle dynamique et répond-elle de manière rapide et efficace à la concurrence sur le marché ?*

- *Fournissez-vous des bonnes pratiques et des ressources pour suivre les dépenses ?*
- *Fournissez-vous des bonnes pratiques et des ressources pour l'optimisation des coûts ?*

Transparence de la tarification
*En raison de la tendance à la baisse constante de la tarification dans les technologies de cloud commercial, due à l'innovation et à la concurrence, le coût unitaire de service mesuré du CISP payé par l'**<ORGANISATION>** en vertu de l'accord-cadre ne doit jamais dépasser la tarification unitaire du fournisseur de cloud publiée sur le site Web du fournisseur de cloud, qui est en vigueur au moment où l'unité de service est consommée par le client.*

Budgétisation et alertes/rapports de facturation
*Pour démontrer la livraison et l'utilisation des technologies cloud, les CISP doivent fournir à l'**<ORGANISATION>** les outils nécessaires pour générer des rapports de facturation détaillée, qui répartissent les coûts par heure, jour ou mois ; par compte dans une organisation ; par produit ou ressources de produit ; ou par balises définies par le client. L'**<ORGANISATION>** reconnaît que, dans le cadre du modèle de responsabilité partagée du cloud, l'**<ORGANISATION>** sera responsable de l'utilisation des fonctionnalités et outils de budgétisation et de facturation fournis par le CISP afin de respecter les exigences uniques de prévision et de génération de rapports.*

- *Fournir des informations sur la manière dont l'**<ORGANISATION>** peut consulter les informations de facturation aux niveaux global et granulaire, en visualisant les schémas de dépenses des ressources CISP au fil du temps, en plus de prévoir les dépenses futures.*
- *Fournir des informations quant à la manière dont l'**<ORGANISATION>** peut filtrer la vue d'utilisation/de facturation par service, par compte associé ou par balises personnalisées appliquées aux ressources, et créer des alertes de facturation qui envoient des notifications lorsque l'utilisation des services approche des seuils/budgets définis par l'<**ORGANISATION**> ou les dépasse.*
- *Fournir des informations quant à la manière dont l'**<ORGANISATION>** peut prévoir la quantité de services cloud utilisée sur une période définie, en fonction de l'utilisation passée. Le CISP doit proposer une **estimation** de la facture du CISP pour l'**<ORGANISATION>** et permettre à l'**<ORGANISATION>** d'utiliser des alarmes et des budgets pour les montants prévus, afin d'avoir une gouvernance supérieure sur les coûts et les dépenses.*

2.4.2 Comparaison entre les fournisseurs

Les organisations du secteur public exigent souvent une compétition entre les soumissionnaires à l'aide de critères d'évaluation tels que la meilleure valeur, l'offre la plus avantageuse économiquement (MEAT, Most Economically Advantageous Tender) ou le prix le plus bas. Lors de la planification du tarif des contrats exécutoires ou mini compétitions d'accord-cadre, il est important de créer une approche prenant en compte les fonctionnalités uniques du cloud. Par exemple, il faut comprendre que la simple comparaison des postes entre les offres des fournisseurs de cloud (par ex. serveur / instance ou stockage) n'est pas un moyen de comparaison efficace, car il ne prend pas en compte les fonctionnalités telles que la performance, l'optimisation des coûts grâce aux services natifs cloud et outils de supervision du CISP, ni les services de différenciation que les CISP peuvent proposer gratuitement. De plus, le prix catalogue d'un CISP peut contenir des dizaines de milliers de postes ; les modèles de tarification varient d'un service et d'un fournisseur à un autre.

Analyser le TCO

Nous recommandons de privilégier le coût total de possession (TCO) de cas d'utilisation définis, qui prend en compte tous les aspects d'une solution de cloud (y compris les services de partenaires, les remises CISP standardisées, les caractéristiques techniques qui peuvent améliorer les performances et réduire/optimiser les coûts, etc.).

Comparer des scénarios

Le processus d'évaluation peut également tenir compte des scénarios typiques qui correspondent aux systèmes ou applications courants. Ces scénarios (comme l'hébergement web ou l'implémentation d'un système de ressources humaines avec « x » utilisateurs, etc.) peuvent inclure des variables telles que la vitesse et l'échelle des ressources, les performances de l'application ou de la solution, les délais d'accès au stockage, les données complexes à faible volume contre les tâches de calcul simples à volume élevé, etc. Les applications ou systèmes peuvent également avoir des scénarios classiques, comme le traitement d'un volume élevé lors de la déclaration de revenus ou des notifications d'urgence comme des alertes d'inondation. Les scénarios doivent être complets de manière à inclure la portée de la technologie et des services que le client est susceptible d'utiliser au cours du projet. Ainsi, le client peut comparer le coût global estimé du projet.

Comparer les scénarios financièrement et techniquement

Il est également important de prendre en compte les avantages techniques lors de la comparaison de la tarification entre les offres de CISP. Par exemple, un CISP peut permettre aux clients de créer une topologie de reprise après sinistre (DR, Disaster Recovery) active-active grâce à son modèle intégrant des Datacenters dans des clusters au sein d'une région géographique. Un CISP qui ne possède pas ce type de redondance et de configuration de Datacenter peut être x % plus cher, si l'on tient compte du coût de reprise après sinistre. La solution de comparaison simple ci-dessous montre pourquoi une approche holistique de la tarification, tenant compte des caractéristiques techniques supplémentaires, est essentielle pour évaluer les CISP.

Exemple : un client veut comparer le prix du stockage d'objet fourni par des CISP qualifiés sur un accord-cadre. Le prix de l'« unité » de stockage du CISP 1 est de 0,023 €/Go. Le prix de la même « unité » pour le CISP 2 est de 0,01 €/Go. Dans une simple comparaison unité à unité, le client ne poserait pas des questions essentielles telles que :

1. Combien de copies redondantes de l'objet sont disponibles en cas de défaillance ? Dans l'exemple ci-dessus, le CISP 1 est conçu pour faire face à une perte de données simultanée sur deux sites différents tout en conservant plusieurs copies des données. Dans le cas du CISP 2, aucune copie redondante n'est effectuée.
2. Quel est le niveau de durabilité des objets stockés ? Il est de 99,999999999 % pour le CISP 1 et de 99 % pour le CISP 2.
3. Tenez compte du coût global sur la durée de propriété du projet ou de l'application, et de la manière dont les fonctionnalités d'optimisation des coûts peuvent réduire les coûts concernant le stockage et l'utilisation des données (par exemple, l'augmentation de l'utilisation de fonctions sans serveur d'un CISP peut réduire les coûts de x %).

Il ne s'agit que de quelques-unes des autres considérations techniques à prendre en compte dans la tarification, en particulier concernant la sécurité et la conformité.

Éléments à prendre en compte dans les scénarios de tarification

Tarifs de base : il s'agit essentiellement des tarifs publics des CISP. Les CISP doivent fournir ces prix publiquement ; cependant, comme indiqué ci-dessus, pour comparer efficacement les CISP, les clients peuvent par exemple demander à tous les fournisseurs de donner leurs tarifs pour 3 à 5 scénarios spécifiques (ou le nombre approprié pour le client). Les scénarios doivent être complets et inclure l'étendue des services et technologies que le client est susceptible d'utiliser au cours du projet. Ainsi, le client peut comparer le coût global estimé du projet. Les comparaisons effectuées au niveau du poste/du SKU ont tendance à être plus problématiques qu'utiles pour les clients et les fournisseurs (les clients devraient comparer des dizaines de milliers de postes pour tous les CISP et les fournisseurs devraient fournir ce niveau de détail et le gérer lorsque le prix réel est uniquement déterminé par la consommation de service).

L'évaluation de l'ensemble des capacités fondamentales d'un CISP est essentielle pour les clients cloud qui cherchent à obtenir la meilleure valeur. Par exemple, les CISP peuvent proposer un certain nombre de services gratuits ou principalement gratuits, et l'évaluation de la tarification doit prendre en compte ces services, ainsi que le fait que d'autres CISP puissent facturer des fonctionnalités similaires.

Les critères d'évaluation peuvent être rédigés de manière à permettre aux CISP de faire appel à leurs fonctionnalités « incluses par défaut », et la façon dont ces services exercent un impact global sur les coûts. Les critères d'évaluation peuvent également porter sur la tarification du CISP en fonction du volume/niveau et les remises disponibles commercialement, comme les instances réservées/instances Spot. Par exemple :

- x % d'économies si les clients achètent une capacité de serveur / instance réservée (1 an, 3 ans, etc.)
- x % de remise sur la tarification en fonction du volume
- x % d'économies d'après les révisions de l'architecture et l'optimisation de l'infrastructure, comme le basculement vers une option de serveur / instance mieux adaptée
- Comme indiqué ci-dessus, prenez en compte le coût global sur toute la durée du contrat et la façon dont les fonctions d'optimisation des coûts peuvent réduire les coûts

SCÉNARIO DE TARIFICATION

Les soumissionnaires doivent fournir une tarification pour le scénario ci-dessous, uniquement à des fins d'évaluation. Le prix réel s'appuiera sur la consommation des services, selon un modèle de paiement à l'utilisation et à la demande.

Les exigences représentatives aux fins de découverte de tarif figurent ci-dessous. Il est explicitement entendu qu'au cours de la durée du contrat, ces exigences nominales changeront. Indiquez la tarification pour une capacité réservée de 12 et 36 mois et une capacité à la demande de 12 et 36 mois.

Indiquez :

- *Le nom de la ou des solutions proposées :*
- *La meilleure tarification du soumissionnaire :*
- *Les heures de service : 24 h/24, 7 j/7, 365 j/365*
- *Disponibilité des services : 99,95 %*

Les scénarios de tarification peuvent également inclure des exemples de clients existants possédant des applications similaires, qui ont optimisé leurs dépenses sur 1/2/3 an(s), grâce à l'utilisation des outils de supervision et d'optimisation du CISP, en adoptant des solutions natives cloud optimisées, et grâce à des réductions du prix du CISP.

2.5 Configuration de l'exécution du contrat/Conditions générales

Les technologies et opérations cloud fournies par le CISP sont standardisées de base. Les conditions contractuelles le sont donc également. Cependant, il est possible d'adapter légèrement ces contrats en fonction des contextes législatifs et réglementaires locaux.

Souvent, les méthodes d'approvisionnement informatique traditionnelles comprennent des règles strictes qui exigent que les candidats respectent un grand nombre ou la totalité des exigences de l'approvisionnement, sous peine d'être rejetés. Elles peuvent également inclure un sous-ensemble strict d'exigences obligatoires. Lorsque ce type de méthode d'approvisionnement est utilisé avec les technologies cloud, qui sont en fait un ensemble de composants et outils standardisés vous aidant à concevoir une solution personnalisée, les approvisionnements ont tendance à échouer.

2.5.1 Conditions générales

La première étape en termes de contrat dans un AO de services de cloud consiste à lire et comprendre les conditions commerciales existantes du CISP, qui sont souvent disponibles publiquement sur son site web. Les entités du secteur public acceptent de plus en plus les conditions commerciales des CISP. Une partie des efforts visant à comprendre les conditions consiste à rencontrer les CISP et leurs partenaires pour approfondir leurs approches. La question essentielle est de savoir pourquoi les CISP utilisent des conditions spécifiques. Certaines de ces conditions peuvent paraître différentes des conditions informatiques traditionnelles, mais elles font partie d'un contrat cloud pour des raisons très spécifiques. Si les conditions publiquement disponibles ne sont pas acceptables, les CISP peuvent souvent proposer des contrats légèrement modifiés pour les entreprises clientes.

En plus de lire les conditions générales du CISP, il est important de comprendre les politiques, réglementations et/ou lois existantes (par ex., impliquant la technologie, la classification des données, la confidentialité, le personnel, etc.). Souvent, il existe des politiques/réglementations/lois conçues pour l'achat et l'utilisation d'offres informatiques traditionnelles, qui peuvent ne pas être adaptées au modèle d'un CISP. Par exemple, autoriser uniquement l'utilisation des technologies cloud incluses dans l'offre d'accord-cadre originale via l'AO de services de cloud. Les CISP ajoutent constamment de nouveaux services et de nouvelles fonctionnalités. Pour le client final, il n'est pas logique d'éliminer l'accès à ces nouveaux services uniquement parce que vous suivez une approche d'actualisation de produit informatique traditionnelle. Si tel est le cas, il est important de tenir des discussions approfondies avec les CISP, notamment pour étudier ces politiques/réglementations et/ou lois.

Tirer parti des discussions en amont d'un AO

Comme indiqué ci-dessus, avant de créer la version préliminaire d'un AO, prenez le temps de rencontrer les CISP et les fournisseurs associés pour comprendre leurs conditions générales et les former sur l'approche, les politiques, les réglementations et les lois de votre entité. La partie la plus importante de ces discussions pour les deux parties est de comprendre « pourquoi » les conditions concernées fonctionnent ainsi. Par exemple, les conditions générales du cloud sont différentes des conditions du Datacenter, des services managés, du matériel, des logiciels prêts à l'emploi et de l'intégration système traditionnels. Leurs modèles commerciaux, uniques et impliquant une innovation constante, requièrent que le processus de l'AO soit suffisamment flexible pour permettre des négociations ou des discussions en vue d'une clarification.

En se donnant les moyens de clarifier les conditions générales grâce à des discussions ou à des négociations, les organisations du secteur public acquièrent une meilleure compréhension des modèles de cloud et évitent de rejeter les fournisseurs qui auraient en fait pu répondre à leurs besoins. Dans l'un des processus typiques, l'organisation identifie à l'avance certaines conditions qu'elle veut évoquer et négocier avant de faire son choix. En négociant à l'avance des conditions acceptables avec le ou les soumissionnaires, l'organisation veille à obtenir l'offre la plus adaptée et règle les différends qui pourraient autrement causer le rejet d'une proposition adaptée. Les entités du secteur public peuvent également consulter leurs politiques, réglementations et lois, et les deux parties peuvent comprendre comment l'utilisation du cloud s'adaptera à ces modèles. Souvent, les clauses existantes peuvent être utilisées. Cependant, si un domaine pose problème, les deux parties peuvent collaborer pour trouver une solution (il est préférable d'avoir ces discussions bien avant un AO et la négociation contractuelle).

Flexibilité de la négociation

Pour pouvoir signer des contrats conformes à la législation locale, tout en s'appuyant sur les conditions contractuelles standardisées par le CISP, il est recommandé (1) de demander aux candidats leur contrat standard, (2) de ne pas promulguer des conditions contractuelles non adaptées lors de la définition de l'accord-cadre pour l'AO de services de cloud, et (3) de fournir une option de négociation sur toutes les dispositions de la consultation et des propositions, qui aboutiront à l'accord-cadre (à l'exception des clauses obligatoires en vertu de la loi, naturellement).

NB : la portée de la responsabilité partagée est inhérente au modèle de cloud et doit être prise en compte dans les conditions du contrat (par ex., le CISP confirme que les clients possèdent leurs données, indique leur localisation et fournit des outils pour veiller à ce que le choix des localisations de données soit limité - MAIS - il appartient au client ou au partenaire d'utiliser ces outils).

Notez qu'il est important d'avoir des ***ensembles distincts de conditions générales*** *de contrat pour chacun des LOTS d'un accord-cadre de cloud. Une approche unique pour les contrats de tous les LOTS créerait des problèmes en termes de faisabilité technique et de compatibilité.*

Comme indiqué précédemment, les AO qui comprennent des conditions obligatoires non négociables sont principalement une proposition « à prendre ou à laisser » pour les fournisseurs, ce qui peut entraîner le refus d'une offre autrement acceptable. Les organisations du secteur public doivent soigneusement étudier les conséquences liées à l'utilisation de conditions obligatoires, sauf si la loi l'exige. Les organisations doivent être certaines qu'une exigence ou condition est obligatoire, car les négociations futures sont conditionnées par cette classification. L'utilisation d'exigences ou de conditions obligatoires doit se limiter au strict minimum, afin que l'organisation dispose de la flexibilité nécessaire pour acquérir la meilleure technologie et solution.

N'oubliez pas que les technologies cloud des CISP sont entièrement standardisées et livrées de manière entièrement automatisée. Un CISP ne peut donc pas apporter de modifications aux conditions générales qui nécessiteraient une personnalisation de service sous-jacente. De plus, les prix des services sont généralement publics et standardisés pour tous les utilisateurs. Un CISP ne peut donc pas ajuster la tarification afin d'assumer plus de risque pour un client en particulier.

Achats indirects

Une autre possibilité consiste à acheter des technologies cloud auprès d'un revendeur CISP au lieu de les acheter directement auprès d'un CISP. Vous trouverez plus d'informations sur les revendeurs CISP dans la section *2.1.3* ci-dessus.

Exemple de texte d'AO : conditions générales

*Les CISP ou revendeurs doivent mettre publiquement leurs conditions générales à disposition et donner des informations sur les conditions générales essentielles fournies par l'<**ORGANISATION**>.*

*L'<**ORGANISATION**> entend conclure un contrat écrit avec le soumissionnaire choisi d'après les conditions contractuelles de ce dernier. Le soumissionnaire doit fournir un ensemble de conditions contractuelles proposées pour révision par l'<**ORGANISATION**>, représentant sa meilleure proposition commerciale et juridique. Les soumissionnaires et l'<ORGANISATION> peuvent discuter des ensembles de conditions générales au cours de la phase de <DISCUSSION/NÉGOCIATION>.*

- *Les conditions globales de haut niveau du cadre comporteraient au maximum les éléments suivants :*
  - *Durée du cadre*
  - *Gouvernance du cadre*
  - *Performances du cadre*
  - *Résiliation du cadre*
  - *Portée du cadre*
  - *Processus de commande*
  - *Dispositions de confidentialité*
  - *IP et informations spécifiques à la catégorie*
  - *Exigences techniques minimales à respecter par les CISP, par ex. standard de qualité, accréditation, sécurité et protection des données*
- *Chacun des lots de l'accord-cadre comportera des conditions différentes*
- *Les spécificités du service du CISP peuvent être étudiées et seront traitées lors du contrat exécutoire*
- *Autoriser les modifications du contrat : les conditions ne doivent pas contraindre les clients et les fournisseurs à accepter des modifications du contrat, à ajouter de nouveaux services ou améliorations. La nature évolutive des services de cloud est telle que les améliorations de services deviendront disponibles de manière permanente, ce qui peut permettre d'apporter plus d'efficacité aux clients.*
- *Les accords de niveau de service (SLA) ne doivent pas être spécifiés par le client. Les conditions du client ne doivent pas définir des SLA spécifiques à la commission et personnalisés qui diffèrent des modèles de prestation de service standard des CISP. Si les SLA standard des CISP sont autorisés, ces derniers pourront maintenir des coûts faibles et en faire bénéficier les clients, tout en leur garantissant qu'ils peuvent respecter les SLA.*
- *Les plafonds de responsabilité doivent être proportionnels. La responsabilité doit être proportionnelle aux services achetés et les plafonds de responsabilité ne doivent pas être démesurément élevés. Si les plafonds sont démesurément élevés, les CISP ne seraient plus intéressés par des projets de faible valeur. Ces projets servent souvent d'introduction utile et de « tests » pour les clients, afin de déterminer si certaines solutions de cloud sont efficaces pour leur organisation.*
- *Les clients doivent posséder leurs propres données. Les clients doivent contrôler et posséder leurs données, et être en mesure de déterminer la localisation géographique où elles sont conservées. Cela permettra aux clients d'éviter l'enfermement du fournisseur et de déplacer librement les données vers de nouveaux fournisseurs.*

2.5.2 Comment faire un choix parmi les bénéficiaires par projet

Les organismes du secteur public qui font partie du cadre peuvent commander ou annuler les services en cas de besoin. La conclusion d'un contrat exécutoire en vertu d'un accord-cadre permet aux acheteurs d'affiner leurs exigences en ajoutant des spécifications fonctionnelles pour une annulation, tout en conservant les avantages offerts par l'accord-cadre.

Si nécessaire, une mini compétition peut être organisée afin d'identifier le meilleur fournisseur pour une application ou un projet en particulier. Au cours d'une mini compétition, un client ouvre la compétition en vertu du cadre et invite tous les fournisseurs d'un lot à répondre à un ensemble d'exigences. Le client invitera tous les fournisseurs aptes dans le lot à faire une offre, ce qui souligne l'importance des exigences minimales pour les bénéficiaires d'un AO de services de cloud : elles garantissent un grand nombre d'options pour chaque lot.

Veuillez noter à nouveau qu'il est important d'avoir un ensemble distinct de conditions générales de contrat pour chacune des catégories de lot de type d'offre (par ex. IaaS/PaaS public, IaaS/PaaS communautaire, IaaS/PaaS privé), car une approche unique du contrat pour chaque lot causera des problèmes en termes de faisabilité technique et de compatibilité.

Consultez la section *2.1.4* pour voir un exemple de texte d'AO concernant le choix du bénéficiaire.

2.5.3 Intégration et départ

L'un des éléments à prendre en compte lors de la mise en place d'un accord-cadre de cloud est l'option de système d'achat dynamique (DPS, Dynamic Purchasing System). Avec un modèle DPS, tous les fournisseurs qui respectent les exigences minimales de l'accord-cadre seront admis dans le cadre. Il n'existe pas de limite fixe au nombre de fournisseurs pouvant rejoindre le cadre, et contrairement au modèle de cadre traditionnel, les fournisseurs peuvent également demander à rejoindre le cadre DPS à tout moment au cours de sa durée de vie.

Nous recommandons fortement aux entités du secteur public de définir des standards élevés afin de garantir la qualité et l'assurance du service par des fournisseurs qualifiés, tout en n'étant pas trop spécifiques, afin d'éviter de disqualifier des CISP d'une manière non équitable. En fin de compte, l'objectif est d'éviter de saturer l'utilisateur final avec un grand nombre d'options, tout en conservant un standard élevé pour les technologies cloud disponibles.

3.0 Meilleures pratiques/Leçons apprises

Nous présentons ci-dessous certaines de nos expériences relatives à la réalisation d'un accord-cadre de cloud réussi, avec un AO de services de cloud bien rédigé.

3.1 Gouvernance du cloud

La gouvernance dans le cloud est une responsabilité partagée. Les CISP fournissent des fonctions et services pour intégrer la gouvernance du cloud à tous les aspects d'un environnement de cloud, alors que les clients fournissent leurs standards existants de gouvernance du cloud et apprennent en quoi le cloud facilite la gouvernance du cloud.

Dans le cloud, les clients peuvent créer l'environnement informatique qu'ils souhaitent au lieu de se contenter de gérer celui qu'ils possèdent déjà. Le cloud permet aux clients de : (1) faire l'inventaire complet

de toutes les ressources informatiques ; (2) centraliser la gestion de toutes ces ressources et (3) créer des alertes concernant leur utilisation/facturation/sécurité/etc. Tous ces avantages essentiels du cloud permettent aux clients d'avoir une architecture optimisée (et dans la mesure du possible, automatisée) sans avoir à continuellement fournir et installer un nouveau matériel. C'est le CISP qui s'en charge, ce qui permet aux clients de ne plus devoir gérer une infrastructure globale et de reporter toute leur attention sur leur activité stratégique.

Le côté pratique d'un cloud de CISP réside dans son système API très important. Pour lancer un nouveau serveur ou changer des paramètres de sécurité, il suffit d'effectuer des appels d'API. Toute modification dans l'environnement est consignée et enregistrée (l'auteur, l'objet, le lieu et le moment de chaque modification). Cela permet une gouvernance cloud, un contrôle et une visibilité qui sont uniquement possibles dans un environnement de cloud. Cela permet aux clients de repenser les modèles de gouvernance informatique existants et de déterminer comment ils peuvent être simplifiés et améliorés, compte tenu des avantages qu'apporte le cloud.

La gouvernance du cloud peut également consister à communiquer et à intégrer les changements de processus positifs, ainsi que les nouveaux ensembles de compétences livrés avec le cloud. Par exemple, les chefs de projet sont habitués à attendre pendant des mois qu'un environnement informatique soit créé, et peuvent de ce fait fortement surestimer les délais pour créer un environnement de développement ou de test dans le cloud (ce qui peut ne prendre que quelques minutes). L'ajustement à cette nouvelle capacité d'adaptation sera un processus évolutif, programme par programme. Ces expériences doivent être partagées afin qu'un accord-cadre de cloud puisse continuer à évoluer, de façon à aligner les exigences aux nouveaux processus et à la capacité d'adaptation.

3.2 Budgétisation pour le cloud

Concernant la structure de tarification du cloud en paiement à l'utilisation pour répondre aux exigences de budgétisation et d'acquisition du secteur public, nous avons déterminé qu'il est utile de regrouper les services CISP en un seul poste (serveur / instance, stockage, mise en réseau, base de données, IoT, etc.), nommé Technologies cloud. Cette approche offre de la flexibilité pour proposer toutes les technologies CISP actuelles et nouvelles aux utilisateurs en temps réel, et fournit aux utilisateurs un accès rapide aux ressources dont ils ont besoin, quand ils en ont besoin. Elle s'adapte également aux fluctuations de la demande , pour une utilisation optimisée et des faibles coûts.

Les organisations du secteur public peuvent ajouter des postes pour les commandes d'autres lots dans un cadre cloud, si elles ont besoin de services de consulting/professionnels ou managés, de logiciels d'une marketplace, de services de support cloud et d'une formation sur les offres du CISP.

Une flexibilité de contrat supplémentaire peut être offerte en employant des postes de contrat facultatifs dans les catégories de ressources appropriées, afin de s'adapter à la croissance future. Autrement, si une organisation souhaite associer les technologies cloud à des services de consulting/professionnels/managés en un seul poste, il est possible de créer un poste « Technologies cloud et tâches auxiliaires ».

Voici ci-dessous un exemple représentatif de cette approche. Dans cet exemple, chaque unité du poste « #1001 - Technologies cloud » est égale à 1,00 € de « Technologies cloud » utilisées. Chaque mois, les augmentations de commande peuvent être financées d'après les projections d'utilisation actuelles et planifiées.

Tableau 3 - Exemple de structure de tarification de poste unique.

N° D'ARTICLE	RESSOURCES/SERVICES	QUANTITÉ	UNITÉ	PRIX UNITAIRE	MONTANT
1001	Technologies cloud	1 000	Chacun	1 €	1 000 €
1002	Services de consulting	1	Par semaine	3 000 €	3 000 €
1003	Support cloud	1	Par mois	1 000 €	1 000 €
1004	Formation cloud	1	Par jour	3,00 €	3 000 €
1005	Marketplace cloud	10	Chacun	10 €	100 €

Exemple de fonctionnement de cette structure : une organisation du secteur public contacte un CISP pour estimer la quantité de services de technologies cloud qui sera utilisée par l'organisation. L'organisation accepte les conditions du fournisseur de 10 millions € sur 5 ans, ce qui revient à 2 millions € par an. L'organisation s'engage à verser le montant annuel initial de 2 millions €. Chaque mois, une facture est émise et des fonds sont prélevés pour la payer. Un prélèvement est effectué sur ce compte. Les fonds restants sont surveillés grâce aux outils de supervision et de prévision du CISP. S'il reste peu de fonds, l'organisation demande des fonds supplémentaires au directeur financier, qui pourront être dédiés au maintien des services.

Exemple de texte d'AO : tarifs - établissement de contrat

CONDITIONS DE PAIEMENT

Les conditions de paiement doivent être structurées de manière à ne payer que les ressources utilisées par l'<ORGANISATION> comme indiqué ci-dessous :

1. *Le paiement mensuel s'appuiera sur l'utilisation/la consommation réelle des services et selon la tarification disponible publiquement du CISP.*

GARANTIE MINIMALE ET DÉPENSES MAXIMALES

Il est impossible pour l'<ORGANISATION> de déterminer exactement quel volume de ressources d'un fournisseur de services de cloud spécifique sera consommé sur une période donnée. Les commandes devront donc être spécifiées en tant que quantités unitaires à prix fixe d'un seul poste de commande pour « Technologies cloud ».

Chaque unité du poste commandé sera équivalente à <1,00 €> de technologies cloud commandées. Des commandes incrémentielles seront passées de temps à autre en modifiant cette commande, en différentes quantités, pour permettre à l'<ORGANISATION> de précommander différentes quantités « montant en euros » de technologies cloud CISP d'après l'utilisation estimée pour les besoins de différentes durées. Les quantités seront précommandées de temps à autre par l'<ORGANISATION> selon des montants suffisants pour couvrir le coût estimé des technologies cloud qui seront utilisées pour répondre à différentes exigences.

N° d'article	Description	Qté	Unité	Prix
01	Technologies cloud CISP	1 000	Chacun	1 000 €

MINIMUM DE COMMANDE/COMMANDE INCRÉMENTIELLE

Les commandes seront passées de temps à autre pour différentes quantités de <10 000> unités de poste en fonction de l'utilisation estimée des technologies cloud par l'<ORGANISATION>. Ces dispositions offriront à l'<ORGANISATION>

*la flexibilité nécessaire pour précommander **<10 000>** unités de « technologies cloud » selon le besoin, afin de poursuivre les opérations et d'assurer la cohérence avec les pratiques commerciales de « paiement à l'utilisation » du cloud computing.*

*Un incrément initial de **<100 000>** unités au coût de **<100 000 €>** sera commandé lors de la conclusion du contrat exécutoire. Le nombre minimum d'unités de postes totales qui peut être commandé dans une seule commande incrémentielle en utilisant un ou plusieurs postes est de **<x>.** Le nombre maximum d'unités pouvant être commandé dans la commande de livraison ne peut pas dépasser **<x>,** mais ne doit jamais dépasser la valeur du contrat exécutoire lorsqu'il est associé à toutes les unités précédentes commandées. Il revient à l'**<ORGANISATION>** de s'assurer que toutes les commandes respectent les limites spécifiées dans cette section.*

MAXIMUM DE COMMANDE
*La valeur totale maximale de commande atteint **<x>** et se compose de jusqu'à **< x>** unités d'un seul poste au tarif de **<x>** par unité. La valeur s'appuie sur une estimation des exigences de l'**<ORGANISATION>** sur la période de performance, mais n'est pas garantie.*

3.3 Comprendre le modèle commercial du partenaire

Les entités du secteur public doivent comprendre les modèles selon lesquels les CISP proposent leurs offres, et comprendre que les partenaires qui fournissent des services de consulting, des services managés, des services de revente et plus encore, sont essentiels au processus. De nombreux clients auront besoin d'un fournisseur de cloud pour leur infrastructure et sous-traiteront les tâches bureautiques de planification, de migration et de gestion à un intégrateur de systèmes ou à un fournisseur de services managés. Étant donné que différents services sont impliqués, certaines exigences peuvent ne pas s'appliquer aux fournisseurs de cloud, comme la transmission de certaines clauses à des sous-traitants.

Ces transmissions de clauses permettent de comprendre le fonctionnement des partenaires et des revendeurs en lien avec les CISP. Dans certains types d'approvisionnement, des clauses exigent que le fournisseur principal transmette certaines clauses obligatoires à tous ses partenaires/sous-traitants. En général, les CISP ne proposent pas de partenaires sous-traitants officiels et ne font pas appel à de tels partenaires, car ils proposent un service standardisé à grande échelle qui n'est pas adapté spécifiquement pour répondre aux exigences particulières d'un client final (y compris aux besoins d'un client du secteur public dans le cadre d'un contrat du secteur public). Dans un modèle d'approvisionnement indirect (acquisition de services de cloud via un revendeur CISP), un CISP peut rejeter les clauses de son revendeur, puisqu'elles ne sont pas applicables à un fournisseur de services commerciaux de « second rang ». Dans ce cas, le CISP n'effectue pas lui-même les tâches prévues au contrat ; au lieu de cela, un partenaire du CISP utilise l'infrastructure de ce dernier pour le faire. Le CISP est, par conséquent, un fournisseur commercial (pas un sous-traitant) pour les activités d'un partenaire. Dans un modèle d'approvisionnement direct (achat des services de cloud directement auprès d'un CISP), un CISP rejette en général ces clauses « obligatoires » caractéristiques d'un fournisseur sous-traitant standard de marchandises. Cela tient à la nature commerciale des services contractuels et au fait que la plupart des CISP n'ont pas besoin de sous-traitants pour fournir leurs services commerciaux.

3.4 Courtiers de cloud

Le concept de courtier de cloud pour réduire la possibilité d'enfermement du fournisseur peut être problématique. Bien que les services de courtage de cloud puissent, en théorie, représenter une bonne idée, ils risquent en pratique d'augmenter la complexité et la confusion plutôt que la valeur réalisée.

S'ils tentent de concevoir des applications destinées à fonctionner simultanément ou indifféremment sur différents clouds, il est forcément nécessaire de faire des compromis en termes de capacité (il n'existe pas de logiciel d'apprentissage du langage, tel que Rosetta Stone, pour le cloud). Enfin, cette approche peut ajouter une couche inutile de complexité entre les clients du secteur public et leurs services de cloud, ce qui peut compromettre la rentabilité et les gains de sécurité qu'ils cherchent à obtenir, et limiter l'évolutivité et la flexibilité. Les coûts augmentent et l'innovation ralentit.

3.5 Approvisionnement pré-AO/étude de marché

Lorsqu'une entité du secteur public planifie un AO de services de cloud, elle doit inclure les parties prenantes de tous les aspects de l'organisation : direction, commerce, technologie, finances, approvisionnement, juridique et contrats, dès le début du processus. Cette approche permet de s'assurer que toutes les parties prenantes comprennent le modèle de cloud et bénéficient donc d'une approche éclairée pour réévaluer les méthodes d'approvisionnement informatique traditionnelles.

En termes de dialogue avec le secteur, nous recommandons fortement aux entités du secteur public de prendre le temps d'avoir une conversation approfondie pour recueillir les commentaires du secteur : CISP, partenaires de CISP, fournisseurs de marketplace PaaS/SaaS, et experts du secteur. Par exemple, ce dialogue peut prendre la forme de journées du secteur ou d'ateliers sur la sécurité et l'approvisionnement. Un autre moyen efficace d'acquérir une compréhension approfondie de l'approvisionnement cloud consiste à publier une demande d'informations, ou idéalement, une ébauche d'AO. Souvent, ces documents incluent des problèmes potentiels qui peuvent être identifiés, évoqués et ajustés avant la publication de l'AO de services de cloud finalisé.

Annexe A - Exigences techniques pour la comparaison entre les soumissionnaires

Nous avons répertorié ci-dessous des exigences de technologie cloud génériques qui peuvent être utilisées pour comparer des CISP lors de contrats exécutoires ou de mini compétitions dans un accord-cadre de cloud.

1. Profil de fournisseur cloud

	Exigence
1.	***EXPÉRIENCE DU MARCHÉ :*** *Depuis combien d'années le fournisseur de cloud est-il opérationnel dans le segment de marché du cloud ?*
2.	***OUVERTURE ET PROTECTION DES DONNÉES :*** *Le fournisseur de cloud adhère-t-il à la protection des données ou aux codes de conduite du secteur en matière de réversibilité ? Le fournisseur de cloud adhère-t-il aux principes de développement d'API open source et ouverte ?*

2. Infrastructure mondiale

	Exigence
1.	***PORTÉE MONDIALE :*** *Le fournisseur de cloud offre-t-il une infrastructure mondiale pour aider les utilisateurs à atteindre une faible latence et un débit élevé ?*
2.	***RÉGIONS :*** *Le fournisseur de cloud a-t-il une présence régionale dans les zones géographiques nécessaires ?*
3.	***DOMAINES/ZONES :*** *Le fournisseur de cloud implémente-t-il le concept de domaines ou zones, où plusieurs Datacenters sont regroupés via un réseau à faible latence pour assurer une haute disponibilité et une tolérance aux pannes ?* • *Si oui, veuillez indiquer le nombre de domaines ou zones et le nombre de Datacenters dans les zones géographiques nécessaires.*
4.	***DISTANCE PAR RAPPORT AUX DOMAINES/ZONES :*** *Le fournisseur de cloud crée-t-il ses domaines ou zones avec des Datacenters qui sont physiquement éloignés afin de prendre en charge la redondance, la haute disponibilité et la faible latence ?*
5.	***CENTRES DE DONNÉES CRÉÉS :*** *Le fournisseur de cloud offre-t-il des Datacenters conçus de manière à rester isolés en cas de pannes subies dans d'autres Datacenters, avec une alimentation, une mise en réseau et un refroidissement redondants ?*
6.	***RÉPLICATION DE DATACENTER :*** *Le fournisseur de cloud offre-t-il une réplication des données entre les Datacenters au sein d'un domaine ou d'une zone avec un basculement automatique ?*
7.	***RÉPLICATION DANS LES DOMAINES/ZONES :*** *Le fournisseur de cloud offre-t-il une réplication des données entre les domaines ou zones au sein d'une région ?*

3. Infrastructure.

3.1 Serveur / instance

	Exigence
1.	***SERVEUR / INSTANCE – INSTANCE STANDARD – USAGE GÉNÉRAL :*** *Le fournisseur de cloud offre-t-il les types d'instance suivants ?* • *Usage général : type d'instance optimisé pour les applications génériques et qui fournit un équilibre entre les ressources de serveur / instance, de mémoire et de réseau.* o *Si oui, quelle est la plus grande instance ?*
2.	***SERVEUR / INSTANCE – INSTANCE STANDARD – OPTIMISÉ POUR LA MÉMOIRE :*** *Le fournisseur de cloud offre-t-il les types d'instance suivants ?* • *Optimisé pour la mémoire : optimisé pour les applications qui nécessitent une importante capacité de mémoire.* o *Si oui, quelle est la plus grande instance ?*
3.	***SERVEUR / INSTANCE – INSTANCE STANDARD – OPTIMISÉ POUR LE CALCUL :*** *Le fournisseur de cloud offre-t-il les types d'instance suivants ?* • *Optimisé pour le calcul : optimisé pour les applications qui nécessitent une importante capacité de calcul.* o *Si oui, quelle est la plus grande instance ?*
4.	***SERVEUR / INSTANCE – INSTANCE STANDARD – OPTIMISÉ POUR LE STOCKAGE :*** *Le fournisseur de cloud offre-t-il les types d'instance suivants ?* • *Optimisé pour le stockage : offre une capacité de stockage local importante.* o *Si oui, quelle est la capacité de stockage maximale (c.-à-d. 5, 10, 20, 50 To) et quel est le nombre maximal de disques (HDD/SSD) pouvant être alloué et attaché à une instance ?*
5.	***SERVEUR / INSTANCE – INSTANCE STANDARD – OPTIMISÉ POUR LES APPLICATIONS GRAPHIQUES :*** *Le fournisseur de cloud offre-t-il les types d'instance suivants ?* • *Applications graphiques à faible coût : fournissent une accélération graphique à faible coût aux instances de serveur / instance.* o *Si oui, quelle est la plus grande instance ?*
6.	***SERVEUR / INSTANCE – INSTANCE STANDARD – OPTIMISÉ POUR LES GPU :*** *Le fournisseur de cloud offre-t-il les types d'instance suivants ?* • *GPU : fournit des processeurs graphiques (unités GPU) matériels pour les applications à contenu graphique volumineux.* o *Si oui, combien d'unités GPU et quels modèles d'unités GPU le fournisseur de cloud est-il en mesure de fournir par instance ?*
7.	***SERVEUR / INSTANCE – INSTANCE STANDARD – OPTIMISÉ POUR LES FPGA :*** *Le fournisseur de cloud offre-t-il les types d'instance suivants ?* • *FPGA : ce type d'instance offre des circuits logiques programmables (FPGA) pour développer et déployer des accélérations matérielles personnalisées pour les applications.* o *Si oui, combien de FPGA le fournisseur de cloud est-il en mesure de fournir par instance ?*

8.	*SERVEUR / INSTANCE – INSTANCE À CAPACITÉ EXTENSIBLE :* *Le fournisseur de cloud offre-t-il des instances à capacité extensible qui fournissent un niveau de référence en matière de performances d'unité de traitement centrale (CPU) avec la possibilité de dépasser ce niveau ?* • *Si oui, quelle est la plus grande instance à capacité extensible ?*
9.	*SERVEUR / INSTANCE – INSTANCE À VOLUME D'I/O IMPORTANT :* *Le fournisseur de cloud offre-t-il des instances qui utilisent des disques SSD (Solid State Drive) NVMe (Non-Volatile Memory Express), optimisés pour une faible latence, des performances très élevées en I/O aléatoires et un débit de lecture séquentielle élevé ?* • *Si oui, quelle est la capacité maximale d'opérations d'entrée/sortie par seconde (IOPS) de la plus grande instance ?*
10.	*SERVEUR / INSTANCE – STOCKAGE LOCAL TEMPORAIRE :* *Le fournisseur de cloud prend-il en charge le stockage local pour les instances de calcul à des fins de stockage temporaire d'informations qui changent fréquemment ?*
11.	*SERVEUR / INSTANCE – PRISE EN CHARGE DE PLUSIEURS CARTES RÉSEAUX :* *Le fournisseur de cloud prend-il en charge plusieurs cartes d'interfaces réseau (principales et supplémentaires) à allouer à une instance donnée ?* • *Si oui, quel est le nombre maximal de cartes réseau par instance ?*
12.	*SERVEUR / INSTANCE – AFFINITÉ D'INSTANCES :* *Le fournisseur de cloud offre-t-il aux utilisateurs la capacité de regrouper les instances de manière logique au sein du même Datacenter ?*
13.	*SERVEUR / INSTANCE – ANTI-AFFINITÉ D'INSTANCES :* *Le fournisseur de cloud offre-t-il aux utilisateurs la capacité de regrouper les instances de manière logique et de les placer dans différents Datacenters au sein d'une région ?*
14.	*SERVEUR / INSTANCE – MISE EN SERVICE EN LIBRE-SERVICE :* *Le fournisseur de cloud fournit-il une mise en service en libre-service de plusieurs instances simultanément, par le biais d'une interface par programmation, d'une console de gestion ou d'un portail web ?*
15.	*SERVEUR / INSTANCE – PERSONNALISATION :* *Le fournisseur de cloud fournit-il des instances personnalisables, c.-à-d. la possibilité de modifier les paramètres de configuration tels que les unités de traitement central virtuelles (vCPU) et la mémoire vive disponible (RAM) ?*
16.	*SERVEUR / INSTANCE – LOCATION :* *Le fournisseur de cloud fournit-il des instances à client unique qui s'exécutent sur du matériel dédié à un utilisateur unique ?* • *Si oui, quelle est la plus grande instance à client unique disponible ?*
17.	*SERVEUR / INSTANCE – AFFINITÉ DE L'HÔTE :* *Le fournisseur de cloud offre-t-il la possibilité de lancer une instance et de spécifier que cette instance redémarre toujours sur le même hôte physique ?*
18.	*SERVEUR / INSTANCE – ANTI-AFFINITÉ DE L'HÔTE :* *Le fournisseur de cloud offre-t-il la possibilité de diviser et d'héberger des instances spécifiques sur différents hôtes physiques ?*
19.	*SERVEUR / INSTANCE – SCALABILITÉ AUTOMATIQUE :* *Le fournisseur de cloud offre-t-il la possibilité d'accroître automatiquement le nombre d'instances au cours des pics de demande afin de maintenir les performances (c.-à-d. monter en charge) ?*

20.	***SERVEUR / INSTANCE – MÉCANISME D'IMPORTATION D'IMAGE :*** *Le fournisseur de cloud offre-t-il aux utilisateurs la possibilité d'importer leurs images existantes et de les sauvegarder comme de nouvelles images accessibles en privé et pouvant, à l'avenir, servir à allouer des instances ?* • *Si oui, quels sont les formats pris en charge ?*
21.	***SERVEUR / INSTANCE – MÉCANISME D'EXPORTATION D'IMAGE :*** *Le fournisseur de cloud prend-il en charge la possibilité de prendre une instance existante en cours d'exécution ou une copie d'instance, et de l'exporter dans un format de machine virtuelle ?* • *Si oui, quels sont les formats pris en charge ?*
22.	***SERVEUR / INSTANCE – INTERRUPTION DE SERVICE :*** *Le fournisseur de cloud propose-t-il des mécanismes pour éviter des interruptions ou temps d'arrêt lorsque le fournisseur effectue une opération de maintenance de matériel ou de service au niveau de l'hôte ?*
23.	***SERVEUR / INSTANCE – REDÉMARRAGE D'INSTANCE :*** *Le fournisseur de cloud fournit-il des mécanismes pour redémarrer automatiquement les instances sur un hôte sain en cas de défaillance de l'hôte physique d'origine ?*
24.	***SERVEUR / INSTANCE – NOTIFICATIONS :*** *Dans le cas d'un événement avec calcul résilient, le fournisseur de cloud est-il en mesure d'en informer l'utilisateur ? De plus, l'utilisateur a-t-il la possibilité de choisir de recevoir ou non ce type de communications par le biais de méthodes en libre-service ?*
25.	***SERVEUR / INSTANCE – PLANIFICATION D'ÉVÉNEMENT :*** *Le fournisseur de cloud offre-t-il la capacité de programmer des événements pour les instances de l'utilisateur, comme le redémarrage, l'arrêt, le démarrage ou encore le retrait de l'instance ?*
26.	***SERVEUR / INSTANCE – MÉCANISME DE SAUVEGARDE ET DE RESTAURATION :*** *Le fournisseur de cloud met-il à disposition un mécanisme intégré de sauvegarde et de récupération ?*
27.	***SERVEUR / INSTANCE – MÉCANISME D'INSTANTANÉ :*** *Le fournisseur de cloud met-il à disposition un mécanisme d'instantané manuel ou à la demande ?*
28.	***SERVEUR / INSTANCE – MÉTADONNÉES :*** *Le fournisseur de cloud propose-t-il un service de métadonnées d'instance qui permet aux utilisateurs de définir des paires clé-valeur arbitraires pour l'instance ?*
29.	***SERVEUR / INSTANCE – APPEL DE MÉTADONNÉES :*** *Le fournisseur de cloud propose-t-il un service de métadonnées d'instance qui fournit une interface de programmation d'application (API) que l'instance peut appeler pour trouver des informations la concernant ?*
30.	***SERVEUR / INSTANCE – MÉCANISME D'OFFRE :*** *Le fournisseur de cloud offre-t-il un mécanisme d'offre permettant de proposer une offre pour les instances à coût faible qui peuvent être immédiatement instanciées afin d'héberger les applications non stratégiques ?*
31.	***SERVEUR / INSTANCE – MÉCANISME DE PLANIFICATION :*** *Le fournisseur de cloud propose-t-il un moyen de planifier et de réserver des capacités de calcul supplémentaires sur une base récurrente, c.-à-d. pour des plannings quotidiens, hebdomadaires et mensuels ?*
32.	***SERVEUR / INSTANCE – MÉCANISME DE RÉSERVATION :*** *Le fournisseur de cloud propose-t-il un moyen de réserver des capacités de calcul supplémentaires pour l'avenir (c.-à-d. sur 1, 2, 3 ans, voire plus) ?*
33.	***SERVEUR / INSTANCE – SYSTÈME D'EXPLOITATION LINUX :***

	Le fournisseur de cloud prend-il en charge les deux dernières versions prises en charge à long terme d'au moins une distribution Linux d'entreprise (comme Red Hat, SUSE) et une distribution Linux gratuite couramment utilisée (comme Ubuntu, CentOS et Debian) ?
34.	***SERVEUR / INSTANCE – SYSTÈME D'EXPLOITATION WINDOWS :*** *Le fournisseur de cloud prend-il en charge les deux dernières versions principales de Windows Server (Windows Server 2017 et Windows Server 2016) ?*
35.	***SERVEUR / INSTANCE – PORTABILITÉ DE LICENCE :*** *Le fournisseur de cloud offre-t-il la portabilité de licence et un support ?* • *Si oui, veuillez citer le fournisseur logiciel, les noms, éditions et versions des logiciels concernés.*
36.	***SERVEUR / INSTANCE – LIMITES DE SERVICE :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des limites de service) concernant la section de calcul ci-dessus ?* *Exemple :* *Nombre maximal d'instances par compte* *Nombre maximal d'hôtes dédiés par compte* *Nombre maximal d'adresses IP réservées*

3.2 Mise en réseau

	Exigence
1.	***MISE EN RÉSEAU – RÉSEAUX VIRTUELS :*** *Le fournisseur de cloud prend-il en charge la possibilité de créer un réseau virtuel isolé logique qui représente le propre réseau d'une entreprise dans le cloud ?*
2.	***MISE EN RÉSEAU – CONNECTIVITÉ DANS LA MÊME RÉGION :*** *Le fournisseur de cloud prend-il en charge la connexion de deux réseaux virtuels au sein de la même région pour acheminer le trafic entre eux à l'aide d'adresses IP (Internet Protocol) privées ?*
3.	***MISE EN RÉSEAU – CONNECTIVITÉ DANS DES RÉGIONS DIFFÉRENTES :*** *Le fournisseur de cloud prend-il en charge la connexion de deux réseaux virtuels entre des régions différentes pour acheminer le trafic entre eux à l'aide d'adresses IP (Internet Protocol) privées ?*
4.	***MISE EN RÉSEAU – SOUS-RÉSEAU PRIVÉ :*** *Le fournisseur de cloud offre-t-il la possibilité de créer des réseaux et sous-réseaux virtuels entièrement isolés (privés) dans lesquels des instances peuvent être allouées sans adresse IP (Internet Protocol) publique ou routage Internet ?*
5.	***MISE EN RÉSEAU – PLAGE D'ADRESSES DE RÉSEAUX VIRTUELS :*** *Le fournisseur de cloud prend-il en charge des plages d'adresses IP (Internet Protocol) spécifiées dans la demande de commentaires (RFC) 1918, ainsi que des blocs d'adresse CIDR (Classless Inter-Domain Routing) routables publiquement ?*
6.	***MISE EN RÉSEAU – PLUSIEURS PROTOCOLES :*** *Le fournisseur de cloud prend-il en charge plusieurs protocoles notamment le protocole TCP (Transmission Control Protocol), le protocole UDP (User Datagram Protocol) et le protocole ICMP (Internet Control Message Protocol) ?*
7.	***MISE EN RÉSEAU – AUTO-AFFECTATION DES ADRESSES IP :*** *Le fournisseur de cloud prend-il en charge la possibilité d'affecter automatiquement des adresses IP publiques à des instances ?*

8.	*MISE EN RÉSEAU – ADRESSES IP STATIQUES RÉSERVÉES :* *Le fournisseur de cloud prend-il en charge des adresses IP associées à un compte utilisateur, et non à une instance spécifique ? L'adresse IP doit rester associée au compte jusqu'à ce qu'elle soit libérée explicitement.*
9.	*MISE EN RÉSEAU – PRISE EN CHARGE D'IPV6 :* *Le fournisseur de cloud prend-il en charge le protocole IPv6 (Internet Protocol version 6) au niveau de la passerelle ou de l'instance, et expose-t-il cette fonctionnalité aux utilisateurs ?*
10.	*MISE EN RÉSEAU – PLUSIEURS ADRESSES IP PAR CARTE RÉSEAU :* *Le fournisseur de cloud prend-il en charge la possibilité d'affecter une adresse IP (Internet Protocol) principale et une adresse IP secondaire à une carte d'interface réseau (carte réseau) qui est attachée à une instance donnée ?*
11.	*MISE EN RÉSEAU – PLUSIEURS CARTES RÉSEAU :* *Le fournisseur de cloud prend-il en charge la possibilité d'affecter plusieurs cartes d'interface réseau (carte réseau) à une instance donnée ?*
12.	*MISE EN RÉSEAU – MOBILITÉ DE CARTE RÉSEAU ET D'ADRESSE IP :* *Le fournisseur de cloud prend-il en charge la possibilité de déplacer des cartes d'interface réseau (cartes réseau) ainsi que des adresses IP entre des instances ?*
13.	*MISE EN RÉSEAU – PRISE EN CHARGE DE SR-IOV :* *Le fournisseur de cloud prend-il en charge des fonctionnalités telles que la virtualisation des I/O à racine unique (SR-IOV) pour à la fois améliorer les performances (paquets par seconde - PPS) et réduire la latence et l'instabilité ?*
14.	*MISE EN RÉSEAU - FILTRAGE DES ENTRÉES :* *Le fournisseur de cloud prend-il en charge l'ajout ou la suppression de règles applicables au trafic entrant (entrées) vers les instances ?*
15.	*MISE EN RÉSEAU – FILTRAGE DES SORTIES :* *Le fournisseur de cloud prend-il en charge l'ajout ou la suppression de règles applicables au trafic sortant (sorties) en provenance des instances ?*
16.	*MISE EN RÉSEAU – ACL :* *Le fournisseur de cloud offre-t-il des listes de contrôle d'accès (ACL) pour contrôler le trafic entrant et sortant vers les sous-réseaux ?*
17.	*MISE EN RÉSEAU – PRISE EN CHARGE DES JOURNAUX DE FLUX :* *Le fournisseur de cloud offre-t-il la possibilité de capturer les journaux de flux réseau ?*
18.	*MISE EN RÉSEAU – NAT :* *Le fournisseur de cloud fournit-il un service managé de passerelle de traduction d'adresses réseau (NAT) pour autoriser les instances situées dans un réseau privé à se connecter à Internet ou à d'autres services de cloud, tout en empêchant Internet d'établir une connexion à ces instances ?*
19.	*MISE EN RÉSEAU – VÉRIFICATION DE LA SOURCE/DESTINATION :* *Le fournisseur de cloud a-t-il la possibilité de désactiver les vérifications de source/destination sur les cartes d'interface réseau (cartes réseau) ?*
20.	*MISE EN RÉSEAU – PRISE EN CHARGE DES VPN :* *Le fournisseur de cloud prend-il en charge la connectivité de réseau privé virtuel (VPN) entre le Datacenter de l'utilisateur et lui-même ?*
21.	*MISE EN RÉSEAU – TUNNELS VPN :* *Le fournisseur de cloud prend-il en charge plusieurs connexions de réseau privé virtuel (VPN) par réseau privé ?*
22.	*MISE EN RÉSEAU – PRISE EN CHARGE DES VPN IPSec :*

	Le fournisseur de cloud permet-il aux utilisateurs d'accéder à des services de cloud via un tunnel VPN (réseau privé virtuel) IPsec (Internet Protocol security) ou via un tunnel VPN de protocole SSL via l'Internet public ?
23.	*MISE EN RÉSEAU – PRISE EN CHARGE DU BGP :* *Le fournisseur de cloud utilise-t-il le protocole BGP (Border Gateway Protocol) pour améliorer le basculement entre tunnels VPN IPsec ?*
24.	*MISE EN RÉSEAU – CONNECTIVITÉ PRIVÉE DÉDIÉE :* *Le fournisseur de cloud offre-t-il un service de connectivité direct et privé entre les localisations du fournisseur de cloud et le Datacenter, le bureau ou l'environnement de colocalisation d'un utilisateur permettant ainsi des transferts de données volumineux et rapides ?*
25.	*MISE EN RÉSEAU – ÉQUILIBRAGE DE CHARGE FRONTAL :* *Le fournisseur de cloud fournit-il un service d'équilibrage de charge frontal (accessible sur Internet) qui traite les demandes des clients via Internet et les distribue entre les instances qui sont enregistrées auprès de l'équilibreur de charge ?*
26.	*MISE EN RÉSEAU – ÉQUILIBRAGE DE CHARGE BACKEND :* *Le fournisseur de cloud offre-t-il un service d'équilibrage de charge dorsal (privé) qui achemine le trafic vers des instances hébergées dans des sous-réseaux privés ?*
27.	*MISE EN RÉSEAU – ÉQUILIBRAGE DE CHARGE DE COUCHE 7 :* *Le fournisseur de cloud offre-t-il un service d'équilibreur de charge de couche 7 (HTTP – hypertext transfer protocol) capable d'équilibrer la charge du trafic réseau sur plusieurs instances ?*
28.	*MISE EN RÉSEAU – ÉQUILIBRAGE DE CHARGE DE COUCHE 4 :* *Le fournisseur de cloud offre-t-il un service d'équilibreur de charge de couche 4 (TCP – transmission control protocol) capable d'équilibrer la charge du trafic réseau sur plusieurs instances ?*
29.	*MISE EN RÉSEAU – AFFINITÉ DE SESSION POUR LES ÉQUILIBREURS DE CHARGE :* *Le fournisseur de cloud offre-t-il un service d'équilibrage de charge qui prend en charge l'affinité de session ?*
30.	*MISE EN RÉSEAU – ÉQUILIBRAGE DE CHARGE BASÉ SUR LE DNS :* *Le fournisseur de cloud offre-t-il un service d'équilibrage de charge capable d'équilibrer la charge du trafic vers des instances hébergées sur plusieurs hôtes qui appartiennent à un seul domaine ?*
31.	*MISE EN RÉSEAU – JOURNAUX D' ÉQUILIBRAGE DE CHARGE :* *Le fournisseur de cloud fournit-il des journaux qui capturent des informations détaillées sur toutes les demandes envoyées à un équilibreur de charge ?*
32.	*MISE EN RÉSEAU – DNS :* *Le fournisseur de cloud offre-t-il un service de système de noms de domaine (DNS) hautement disponible et évolutif ?*
33.	*MISE EN RÉSEAU – ROUTAGE DNS BASÉ SUR LA LATENCE :* *Le fournisseur de cloud offre-t-il un service de système de noms de domaine (DNS) qui prend en charge le routage basé sur la latence (c'est-à-dire que le service DNS répond aux requêtes DNS avec les ressources qui fournissent la meilleure latence) ?*
34.	*MISE EN RÉSEAU – ROUTAGE DNS BASÉ SUR LA LOCALISATION GÉOGRAPHIQUE :* *Le fournisseur de cloud offre-t-il un service de système de noms de domaine (DNS) qui prend en charge le routage basé sur la localisation géographique (c'est-à-dire que le service DNS répond aux requêtes DNS en fonction de la localisation géographique des utilisateurs) ?*

35.	*MISE EN RÉSEAU – ROUTAGE DNS BASÉ SUR LE BASCULEMENT :* *Le fournisseur de cloud offre-t-il un service de système de noms de domaine (DNS) qui prend en charge le routage basé sur le basculement (c'est-à-dire que le service DNS achemine les requêtes DNS vers la ressource qui est actuellement active, tandis qu'une seconde ressource attend et ne devient active qu'en cas de défaillance de la ressource principale) ?*
36.	*MISE EN RÉSEAU – SERVICE D'ENREGISTREMENT DE DOMAINES :* *Le fournisseur de cloud offre-t-il des services d'enregistrement de noms de domaine (DNS) (c'est-à-dire que les utilisateurs peuvent rechercher et enregistrer des noms de domaine disponibles) ?*
37.	*MISE EN RÉSEAU – VÉRIFICATIONS DE L'ÉTAT DU DNS :* *Le fournisseur de cloud offre-t-il un service de système de noms de domaine (DNS) qui effectue des vérifications de l'état pour surveiller l'état et les performances des ressources ?*
38.	*MISE EN RÉSEAU – INTÉGRATION DE DNS ET D'ÉQUILIBREUR DE CHARGE :* *Le fournisseur de cloud offre-t-il un service de système de noms de domaine (DNS) qui s'intègre dans l'équilibreur de charge du fournisseur de cloud ?*
39.	*MISE EN RÉSEAU – ÉDITEUR VISUEL :* *Le fournisseur du cloud propose-t-il un outil permettant aux utilisateurs de créer des stratégies de gestion du trafic ?*
40.	*RÉSEAU DE DIFFUSION DE CONTENU (CDN) :* *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) pour diffuser du contenu avec une faible latence et des vitesses de transfert de données élevées ?*
41.	*MISE EN RÉSEAU – EXPIRATION DU CACHE CDN :* *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) qui permet de retirer un objet des caches périphériques avant son expiration, notamment des fonctions telles que l'invalidation d'objets et la gestion des versions d'objet ?*
42.	*MISE EN RÉSEAU – ORIGINES EXTERNES DU CDN :* *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) prenant en charge une origine personnalisée, c'est-à-dire un serveur HTTP (Hypertext Transfer Protocol) ?*
43.	*MISE EN RÉSEAU – OPTIMISATION DU CDN :* *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) avec un contrôle détaillé de la configuration de plusieurs serveurs d'origine et propriétés de mise en cache pour différentes URL (Uniform Resource Locators) ?*
44.	*MISE EN RÉSEAU – CDN GÉO-RESTREINT :* *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) prenant en charge la restriction géographique, c'est-à-dire qui empêche les utilisateurs situés dans des lieux spécifiques d'accéder à du contenu ?*
45.	*MISE EN RÉSEAU – JETONS CDN :* *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) prenant en charge les URL signées qui incluraient généralement des informations supplémentaires telles que la date/heure d'expiration afin de donner aux utilisateurs plus de contrôle sur l'accès à leur contenu ?*
46.	*MISE EN RÉSEAU – CERTIFICATS CDN :*

	Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) prenant en charge les certificats SSL (Secure Sockets Layer) personnalisés afin de diffuser du contenu en toute sécurité via le protocole HTTPS (Hypertext Transfer Protocol Secure) à partir de localisations périphériques ?
47.	***MISE EN RÉSEAU – CACHE CDN MULTICOUCHES :*** *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) qui emploie une méthode de cache multicouches avec l'utilisation de caches périphériques régionaux dans le but de réduire la latence ?*
48.	***MISE EN RÉSEAU – COMPRESSION CDN :*** *Le fournisseur de cloud offre-t-il un service réseau de diffusion de contenu (CDN) qui prend en charge la compression de fichier ?*
49.	***MISE EN RÉSEAU – CHARGEMENTS CHIFFRÉS CDN :*** *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) qui permet aux utilisateurs de charger en toute sécurité leurs données sensibles de manière à ce que ces informations puissent être consultées uniquement par certains composants et services de l'infrastructure d'origine de l'utilisateur ?*
50.	***MISE EN RÉSEAU – POINTS DE TERMINAISON :*** *Le service de mise en réseau du fournisseur de cloud offre-t-il aux utilisateurs des points de terminaison capables d'acheminer le trafic en utilisant la connectivité du réseau interne du fournisseur (c'est-à-dire la connectivité privée) afin de réduire les coûts de communication et d'améliorer la sécurité du trafic ?*
51.	***MISE EN RÉSEAU – LIMITES DE SERVICE :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des limites de service) concernant la section de mise en réseau ci-dessus ?* *Exemple :* *Nombre maximal de réseaux virtuels par compte* *Taille maximale d'un réseau virtuel* *Nombre maximal de sous-réseaux par compte* *Nombre maximal d'équilibreurs de charge par compte* *Nombre maximal d'entrées de liste de contrôle d'accès (ACL)* *Nombre maximal de tunnels de réseau privé virtuel (VPN)* *Nombre maximal d'origines par distribution* *Nombre maximal de certificats par équilibreur de charge*

3.3 Stockage

	Exigence
1.	***SERVICE DE STOCKAGE PAR BLOC :*** *Le fournisseur de cloud offre-t-il des volumes de stockage par bloc à utiliser avec les instances de calcul ?*
2.	***STOCKAGE PAR BLOC – IOPS :*** *Le fournisseur de cloud offre-t-il la possibilité d'acheter une cible de performance ou un niveau de performance explicite sur des volumes de stockage par bloc, comme un certain nombre d'opérations d'entrée/sortie par seconde (IOPS) ou de mégaoctets par seconde (Mo/S) de débit ?*
3.	***STOCKAGE PAR BLOC – DISQUES SSD :*** *Le fournisseur de cloud prend-il en charge les supports de stockage SSD (Solid State Drive) offrant des latences inférieures à 10 millisecondes ?*

	• *Si oui, quel est le nombre maximum de disques SSD pouvant être attachés par instance ?*
4.	*STOCKAGE PAR BLOC – SCALABILITÉ :* *Le fournisseur de cloud offre-t-il aux utilisateurs la possibilité d'augmenter la taille d'un volume de stockage par bloc existant sans devoir allouer un nouveau volume et copier/déplacer les données ?*
5.	*STOCKAGE PAR BLOC – INSTANTANÉS :* *Le fournisseur de cloud dispose-t-il d'une fonctionnalité d'instantané pour son service de stockage par bloc ?*
6.	*STOCKAGE PAR BLOC – SUPPRESSION DES DONNÉES :* *Le fournisseur de cloud prend-il en charge la suppression complète des données de sorte qu'elles ne soient plus lisibles ou accessibles par des utilisateurs non autorisés et/ou des tiers ?*
7.	*STOCKAGE PAR BLOC – CHIFFREMENT DES DONNÉES INACTIVES :* *Le fournisseur de cloud offre-t-il le chiffrement côté serveur des données inactives pour les données stockées sur des volumes et ses instantanés ?* • *Si oui, quel est l'algorithme de chiffrement utilisé ?*
8.	*SERVICE DE STOCKAGE D'OBJETS :* *Le fournisseur de cloud offre-t-il un stockage d'objet « dimensionnable » à volonté, durable et sécurisé pour le stockage et la récupération de tout volume de données à partir du web ?*
9.	*STOCKAGE D'OBJETS – ACCÈS PEU FRÉQUENTS :* *Le fournisseur de cloud propose-t-il un niveau de service de stockage dans le cloud à coût réduit conçu pour stocker les objets et fichiers rarement consultés ?*
10.	*STOCKAGE D'OBJETS – DURABILITÉ INFÉRIEURE :* *Le fournisseur de cloud propose-t-il un niveau de redondance réduite dans lequel l'utilisateur peut stocker des objets non critiques facilement reproductibles à un prix plus bas ?*
11.	*STOCKAGE D'OBJETS – ACCÈS MOINS FRÉQUENTS :* *Le fournisseur de cloud propose-t-il un niveau pour les données plus rarement consultées, mais qui ont quand-même besoin d'un accès rapide ?*
12.	*STOCKAGE D'OBJETS – HIÉRARCHISATION D'OBJET :* *Le fournisseur de cloud propose-t-il une capacité de hiérarchisation du stockage des objets, c'est-à-dire la possibilité de recommander la transition d'un objet entre des classes ou des niveaux de stockage d'objet en fonction de sa fréquence d'accès ?*
13.	*STOCKAGE D'OBJETS – GESTION DU CYCLE DE VIE :* *Le fournisseur de cloud prend-il en charge la gestion du cycle de vie d'un objet à l'aide d'une configuration de cycle de vie qui définit comment les objets sont gérés pendant leur durée de vie, de leur création à leur suppression ?*
14.	*STOCKAGE D'OBJETS – GESTION BASÉE SUR DES STRATÉGIES :* *Le fournisseur de cloud offre-t-il la possibilité de créer et utiliser des stratégies pour gérer les données stockées, leur cycle de vie et leurs paramètres de hiérarchisation ?*
15.	*STOCKAGE D'OBJETS – STRATÉGIES BASÉES SUR LA LOCALISATION ET LA DURÉE :* *Le fournisseur de cloud offre-t-il aux utilisateurs la possibilité de créer des stratégies pouvant restreindre l'accès aux données en fonction de la localisation de l'utilisateur et du moment de la demande ?*
16.	*STOCKAGE D'OBJETS – HÉBERGEMENT DE SITE WEB :* *Le fournisseur de cloud prend-il en charge l'hébergement de sites statiques en dehors de son service de stockage d'objets ?*

17.	***STOCKAGE D'OBJETS – CHIFFREMENT DES DONNÉES INACTIVES :*** *Le fournisseur de cloud prend-il en charge le chiffrement côté serveur (SSE) des données inactives, en gérant les clés de chiffrement ?* • *Si oui, quel est l'algorithme de chiffrement utilisé ?*
18.	***STOCKAGE D'OBJETS – CHIFFREMENT AVEC CLÉS UTILISATEUR :*** *Le fournisseur de cloud offre-t-il des capacités de chiffrement côté serveur (SSE) à l'aide de clés de chiffrement fournies par le client ?*
19.	***STOCKAGE D'OBJETS – SERVICE GÉRÉ PAR CLÉ :*** *Le fournisseur de cloud prend-il en charge le chiffrement côté serveur (SSE) à l'aide d'un service de gestion de clés qui crée des clés de chiffrement, définit les stratégies qui contrôlent la façon dont les clés peuvent être utilisées et contrôle l'utilisation des clés pour prouver qu'elles font l'objet d'une utilisation correcte ?*
20.	***STOCKAGE D'OBJETS – CLÉ PRINCIPALE CÔTÉ CLIENT :*** *Le fournisseur de cloud offre-t-il la possibilité de conserver le contrôle des clés de chiffrement et d'effectuer le chiffrement/déchiffrement d'objets côté client ?*
21.	***STOCKAGE D'OBJETS – COHÉRENCE FORTE :*** *Le fournisseur de cloud prend-il en charge la cohérence en lecture après écriture pour les opérations PUT pour les nouveaux objets ?*
22.	***STOCKAGE D'OBJETS – LOCALITÉ DES DONNÉES :*** *Le fournisseur de cloud offre-t-il un isolement régional fort, de sorte que les objets stockés dans une région ne quitteront jamais cette région, à moins qu'un utilisateur ne les transfère explicitement vers une autre région ?*
23.	***STOCKAGE D'OBJETS – RÉPLICATION :*** *Le fournisseur de cloud offre-t-il une fonction de réplication entre régions qui réplique automatiquement les objets entre des régions sélectionnées par l'utilisateur ?*
24.	***STOCKAGE D'OBJETS – GESTION DES VERSIONS :*** *Le fournisseur de cloud prend-il en charge la gestion des versions, c'est-à-dire la possibilité de stocker et gérer plusieurs versions d'un objet ?*
25.	***STOCKAGE D'OBJETS – MARQUEUR D'ANNULATION DE SUPPRESSION :*** *Le fournisseur de cloud autorise-t-il un utilisateur à marquer un élément comme étant non supprimable ?*
26.	***STOCKAGE D'OBJETS – SUPPRESSION MFA :*** *Le fournisseur de cloud prend-il en charge l'utilisation de l'authentification multifacteurs (MFA) pour les opérations de suppression comme option de sécurité supplémentaire ?*
27.	***STOCKAGE D'OBJETS – CHARGEMENT PARTITIONNÉ :*** *Le fournisseur de cloud autorise-t-il le chargement d'un objet en tant qu'ensemble de parties, où chaque partie est une partie contiguë des données de l'objet, ces parties pouvant être chargées indépendamment et dans n'importe quel ordre ?*
28.	***STOCKAGE D'OBJETS – BALISES :*** *Le fournisseur de cloud offre-t-il la possibilité de créer et associer des balises dynamiques réversibles au niveau des objets ?*
29.	***STOCKAGE D'OBJETS – NOTIFICATIONS :*** *Le fournisseur de cloud offre-t-il la possibilité d'envoyer des notifications quand certains événements se produisent au niveau des objets (par exemple, des opérations d'ajout/de suppression) ?*

30.	***STOCKAGE D'OBJETS – JOURNAUX :*** *Le fournisseur de cloud offre-t-il la possibilité de générer des journaux d'audit comprenant des détails sur une demande d'accès donnée (par exemple, le demandeur, l'heure de la demande, l'action associée à la demande, le statut de réponse et le code d'erreur) ?*
31.	***STOCKAGE D'OBJETS – INVENTAIRE POUR LES OBJETS :*** *Le fournisseur de cloud offre-t-il une capacité d'inventaire des objets pour donner aux utilisateurs la possibilité de consulter rapidement des objets et leur statut afin de permettre une identification immédiate des objets avec un accès public ?*
32.	***STOCKAGE D'OBJETS – INVENTAIRE POUR LES MÉTADONNÉES :*** *Le fournisseur de cloud offre-t-il une capacité d'inventaire des objets pour donner aux utilisateurs la possibilité de consulter rapidement des métadonnées des objets ?*
33.	***STOCKAGE OPTIMISÉ : OPTIMISATION DES CHARGEMENTS :*** *Le fournisseur de cloud a-t-il la possibilité d'acheminer des données à partir de localisations périphériques vers le service de stockage à l'aide d'un chemin réseau optimisé ?*
34.	***STOCKAGE D'OBJETS – CAPACITÉ DE REQUÊTE :*** *Le fournisseur de cloud offre-t-il aux utilisateurs la possibilité d'interroger son service de stockage d'objets à l'aide d'instructions SQL (Structured Query Language) ?*
35.	***STOCKAGE D'OBJETS – EXTRACTION DE SOUS-ENSEMBLE :*** *Le fournisseur de cloud offre-t-il aux utilisateurs la possibilité de récupérer uniquement un sous-ensemble des données à partir d'un objet à l'aide d'expressions SQL (Structured Query Language) simples ?*
36.	***SERVICE DE STOCKAGE DE FICHIER :*** *Le fournisseur de cloud offre-t-il un service de stockage de fichier simple et évolutif à utiliser avec les instances de calcul dans le cloud ?*
37.	***STOCKAGE DE FICHIERS – REDONDANCE :*** *Le fournisseur de cloud stocke-t-il les objets du système de fichiers de manière redondante (par exemple, répertoire, fichier et lien) dans plusieurs Datacenters ou installations pour atteindre de plus hauts niveaux de disponibilité et de durabilité ?*
38.	***STOCKAGE DE FICHIERS – SUPPRESSION DES DONNÉES :*** *Le fournisseur de cloud prend-il en charge la suppression complète des données de stockage de fichier de sorte qu'elles ne soient plus lisibles ou accessibles par des utilisateurs non autorisés et/ou des tiers ?*
39.	***STOCKAGE DE FICHIERS – HAUTE DISPONIBILITÉ :*** *Le système de fichiers géré du fournisseur de cloud offre-t-il un niveau élevé de haute disponibilité ?*
40.	***STOCKAGE DE FICHIERS – NFS :*** *Le fournisseur de cloud prend-il en charge le protocole NFS (Network File System) ?*
41.	***STOCKAGE DE FICHIERS – SMB :*** *Le fournisseur de cloud prend-il en charge le protocole SMB (Server Message Block) ?*
42.	***STOCKAGE DE FICHIER – CHIFFREMENT DES DONNÉES INACTIVES :*** *Le service de stockage de fichiers du fournisseur de cloud prend-il en charge le chiffrement des données inactives ?*
43.	***STOCKAGE DE FICHIERS – CHIFFREMENT DES DONNÉES EN TRANSIT :*** *Le service de stockage de fichiers du fournisseur de cloud prend-il en charge le chiffrement des données en transit ?*

44.	***STOCKAGE DE FICHIERS – OUTIL DE MIGRATION DE DONNÉES :*** *L'outil de migration du fournisseur de cloud offre-t-il un outil de migration de données permettant de transférer des données depuis des systèmes sur site vers le système de fichiers basé sur le cloud ?*
45.	***SERVICE DE STOCKAGE D'ARCHIVES :*** *Le fournisseur de cloud propose-t-il un niveau de service de stockage dans le cloud à coût très bas, conçu pour archiver les objets et fichiers rarement consultés et pratiquement immuables ?*
46.	***STOCKAGE D'ARCHIVES – TOLÉRANCE AUX PANNES :*** *L'architecture du fournisseur de cloud offre-t-elle une tolérance aux pannes pour son service de stockage d'archives ?*
47.	***STOCKAGE D'ARCHIVES – IMMUABILITÉ :*** *Le fournisseur de cloud prend-il en charge l'immuabilité des objets et fichiers archivés ?*
48.	***STOCKAGE D'ARCHIVES – WORM :*** *Le fournisseur du cloud offre-t-il une capacité WORM (Write Once Read Many, une seule écriture et lectures multiples) ?*
49.	***STOCKAGE D'ARCHIVES – EXTRACTION DE SOUS-ENSEMBLE :*** *Le fournisseur de cloud offre-t-il aux utilisateurs la possibilité de récupérer uniquement un sous-ensemble des données à partir d'un objet archivé à l'aide d'expressions SQL (Structured Query Language) simples ?*
50.	***STOCKAGE D'ARCHIVES – VITESSE D'EXTRACTION :*** *Le fournisseur de cloud offre-t-il aux utilisateurs plusieurs options de récupération de données avec différents coûts et durées d'extraction ?*
51.	***STOCKAGE D'ARCHIVES – CHIFFREMENT DES DONNÉES INACTIVES :*** *Le service de stockage d'archives du fournisseur de cloud prend-il en charge le chiffrement de données inactives ?*
52.	***STOCKAGE – LIMITES DE SERVICE :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des limites de service) concernant la section de stockage ci-dessus ?* *Exemple :* *Taille de volume maximum* *Nombre maximal de disques attachés à une instance* *Nombre maximal d'opérations d'entrée/sortie par seconde (IOPS)* *Taille maximum de l'objet* *Nombre maximal d'objets par compte de stockage* *Nombre maximal d'instantanés*

4. Administration

	Exigence
1.	***ADMINISTRATION – UTILISATEURS ET GROUPES :*** *Le fournisseur de cloud offre-t-il un service pour créer et gérer les utilisateurs et les groupes d'utilisateurs de son infrastructure et de ses ressources ?*

2.	***ADMINISTRATION – RÉINITIALISATION DE MOT DE PASSE :*** *Le fournisseur de cloud permet-il aux utilisateurs de réinitialiser leurs propres mots de passe en libre-service ?*
3.	***ADMINISTRATION – AUTORISATIONS :*** *Le fournisseur de cloud offre-t-il la possibilité d'ajouter des autorisations à des utilisateurs et des groupes au niveau des ressources ?*
4.	***ADMINISTRATION – AUTORISATIONS TEMPORAIRES :*** *Le fournisseur de cloud offre-t-il la possibilité de créer des autorisations qui sont valides pendant un intervalle de temps spécifique ?*
5.	***ADMINISTRATION – INFORMATIONS D'IDENTIFICATION TEMPORAIRES :*** *Le fournisseur de cloud offre-t-il aux utilisateurs la possibilité de créer des informations d'identification temporaires et de les fournir à des utilisateurs approuvés, configurées pour une durée de quelques minutes à plusieurs heures ?*
6.	***ADMINISTRATION – CONTRÔLE D'ACCÈS :*** *Le fournisseur de cloud offre-t-il des contrôles précis des accès aux ressources de son infrastructure ?* • *Si oui, quelles conditions peuvent être utilisées par ces contrôles (par exemple, heure du jour, adresse IP d'origine, etc.) ?*
7.	***ADMINISTRATION – STRATÉGIES INTÉGRÉES :*** *L'infrastructure du fournisseur de cloud contient-elle des stratégies de contrôle d'accès intégrées qui peuvent être attachées à des utilisateurs et des groupes ?*
8.	***ADMINISTRATION – STRATÉGIES PERSONNALISÉES :*** *L'infrastructure du fournisseur de cloud autorise-t-elle la création et la personnalisation de stratégies de contrôle d'accès qui peuvent être attachées à des utilisateurs et des groupes ?*
9.	***ADMINISTRATION – SIMULATEUR DE STRATÉGIE :*** *Le fournisseur de cloud offre-t-il un mécanisme pour tester les effets des stratégies de contrôle d'accès avant de valider celles-ci en production ?*
10.	***ADMINISTRATION – AUTHENTIFICATION MFA DU CLOUD :*** *Le fournisseur de cloud prend-il en charge l'utilisation de l'authentification multifacteurs (MFA) comme couche supplémentaire de contrôle d'accès et d'authentification vers son infrastructure ?*
11.	***ADMINISTRATION – LIMITES DE SERVICE :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des limites de service) concernant la section d'administration ci-dessus ?* *Exemple :* *Nombre maximal d'utilisateurs* *Nombre maximal de groupes* *Nombre maximal de stratégies gérées*

5. Sécurité

	Exigence
1.	***SÉCURITÉ – CONTRÔLES DES ANTÉCÉDENTS :*** *L'ensemble du personnel du fournisseur de cloud qui a accès à l'infrastructure du service (physique ou non physique) est-il soumis à des contrôles des antécédents ?*

2.	***SÉCURITÉ – ACCÈS PHYSIQUE :*** *Le fournisseur de cloud restreint-il l'accès du personnel à l'infrastructure du service, sauf en cas de dossier incident spécifique, de demande de modification ou de toute autre autorisation formelle similaire ?*
3.	***SÉCURITÉ – JOURNAUX D'ACCÈS :*** *Le fournisseur de cloud journalise-t-il l'accès du personnel via son infrastructure du service, un tel accès étant systématiquement journalisé et les journaux conservés pendant 90 jours au minimum ?*
4.	***SÉCURITÉ – CONNEXIONS HÔTE :*** *Le fournisseur de cloud restreint-il la connexion du personnel aux hôtes de calcul, plutôt que d'automatiser toutes les tâches effectuées sur les hôtes de calcul, le contenu de ces tâches automatisées étant journalisé et conservé pendant 90 jours au minimum ?*
5.	***SÉCURITÉ – CLÉS DE CHIFFREMENT :*** *Le fournisseur de cloud offre-t-il un service pour créer et contrôler les clés de chiffrement utilisées pour chiffrer les données utilisateur ?*
6.	***SÉCURITÉ – GESTION DES CLÉS D'ACCÈS :*** *Le fournisseur de cloud offre-t-il la possibilité de déterminer quand une clé d'accès a été utilisée pour la dernière fois, de faire tourner les anciennes clés et de supprimer les utilisateurs inactifs ?*
7.	***SÉCURITÉ – CLÉS FOURNIES PAR LE CLIENT :*** *Le fournisseur de cloud permet-il aux utilisateurs d'importer des clés à partir de leur propre infrastructure de gestion des clés vers son service de gestion des clés ?*
8.	***SÉCURITÉ – INTÉGRATION DU SERVICE DE CLÉS DE CHIFFREMENT :*** *Le service gestion des clés du fournisseur de cloud s'intègre-t-il à d'autres services cloud pour fournir une capacité de chiffrement des données inactives ?*
9.	***SÉCURITÉ – HSM :*** *Le fournisseur de cloud offre-t-il des modules de sécurité matériels (HSM, Hardware Security Module) dédiés, c'est-à-dire des dispositifs matériels qui offrent un stockage de clé et des opérations de chiffrement sécurisés au sein d'un module matériel inviolable ?*
10.	***SÉCURITÉ – DURABILITÉ DES CLÉS DE CHIFFREMENT :*** *Le fournisseur de cloud prend-il en charge la durabilité des clés, notamment le stockage de plusieurs copies pour garantir la disponibilité des clés si nécessaire ?*
11.	***SÉCURITÉ – SSO :*** *Le fournisseur de cloud offre-t-il un service d'authentification unique (SSO) géré qui permet aux utilisateurs de gérer de façon centralisée plusieurs comptes et applications métier ?*
12.	***SÉCURITÉ – CERTIFICATS :*** *Le fournisseur de cloud offre-t-il un service managé pour allouer, gérer et déployer des certificats Secure Sockets Layer (SSL)/Transport Layer Security (TLS) ?*
13.	***SÉCURITÉ – RENOUVELLEMENT DES CERTIFICATS :*** *Le service de gestion des certificats du fournisseur de cloud facilite-t-il le renouvellement des certificats ?*
14.	***SÉCURITÉ – CERTIFICATS GÉNÉRIQUES :*** *Le service de gestion des certificats du fournisseur de cloud prend-il en charge l'utilisation des certificats génériques ?*
15.	***SÉCURITÉ – AUTORITÉ DE CERTIFICATION :*** *Le service de gestion des certificats du fournisseur de cloud tient-il également lieu d'autorité de certification (CA) ?*
16.	***SÉCURITÉ – ACTIVE DIRECTORY :***

	Le fournisseur de cloud offre-t-il un service Microsoft Active Directory (AD) géré dans le cloud ?
17.	***SÉCURITÉ – ACTIVE DIRECTORY SUR SITE :*** *Le service Microsoft Active Directory (AD) géré du fournisseur de cloud prend-il en charge l'intégration à l'annuaire Microsoft Active Directory (AD) sur site ?*
18.	***SÉCURITÉ – LADP :*** *Le service Microsoft Active Directory (AD) géré du fournisseur de cloud prend-il en charge le protocole LDAP (Lightweight Directory Access Protocol) ?*
19.	***SÉCURITÉ – ACTIVE DIRECTORY :*** *Le service Microsoft Active Directory (AD) géré du fournisseur de cloud prend-il en charge SAML (Security Assertion Markup Language) ?*
20.	***SÉCURITÉ – GESTION DES INFORMATIONS D'IDENTIFICATION :*** *Le fournisseur de cloud offre-t-il un service managé qui aide les utilisateurs à faire tourner, gérer et récupérer facilement des informations d'identification, comme de clés d'API (interface de programmation d'application), des informations d'identification de base de données et d'autres secrets ?*
21.	***SÉCURITÉ – WAF :*** *Le fournisseur de cloud offre-t-il un pare-feu d'application web (WAF) qui contribue à protéger les applications web contre les attaques web courantes susceptibles d'affecter la disponibilité des applications, de compromettre la sécurité ou de consommer un volume de ressources trop important ?*
22.	***SÉCURITÉ – DDOS :*** *Le fournisseur de cloud offre-t-il un service de protection contre les attaques par déni de service distribué (DDoS) les plus courantes et les plus fréquente du réseau et de la couche de transport, ainsi que la possibilité d'écrire des règles personnalisées pour minimiser les attaques sophistiquées de la couche application ?*
23.	***SÉCURITÉ – RECOMMANDATIONS DE SÉCURITÉ :*** *Le fournisseur de cloud offre-t-il un service pour évaluer automatiquement les failles potentielles dans les applications et les ressources ?*
24.	***SÉCURITÉ – DÉTECTION DES MENACES :*** *Le fournisseur du cloud offre-t-il un service managé de détection des menaces ?*
25.	***SÉCURITÉ – LIMITES DE SERVICE :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des limites de service) concernant la section de sécurité ci-dessus ?* *Exemple :* *Nombre maximal de clés principales client* *Nombre maximal de modules de sécurité matériels (HSM)*

6. Conformité

La liste ci-dessous a été fournie à des fins d'illustration uniquement et ne doit pas être considérée comme exhaustive pour les certifications et standards pouvant s'appliquer aux services cloud.

Veuillez indiquer l'ensemble de normes de conformité internationales et spécifiques du secteur satisfaites par le fournisseur de cloud :

Certifications / Attestations	***Lois, règlementations et confidentialité***	***Adéquations / Infrastructures***

☐ *C5 [Allemagne]*	☐ *Directive sur la protection des données dans l'UE*	☐ *CDSA*
☐ *Code de conduite sur la protection des données CISPE*	☐ *Clauses types de l'UE*	
☐ *DIACAP*	☐ *FERPA*	☐ *CIS*
☐ *DoD SRG niveaux 2 et 4*	☐ *RGPD*	☐ *Informations sur la justice pénale. Service (CJIS)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *Bouclier de protection des données UE – États-Unis*
☐ *HDS (France, Santé)*	☐ *HITECH*	☐ *Safe Harbor UE*
☐ *ISO 9001*	☐ *IRS 1075*	☐ *FISC*
☐ *ISO 27001*	☐ *ITAR*	☐ *FISMA*
☐ *ISO 27017*	☐ *PDPA – 2010 [Malaisie]*	☐ *G-Cloud [Royaume-Uni]*
☐ *ISO 27018*	☐ *PDPA – 2012 [Singapour]*	☐ *GxP (FDA CFR 21 Partie 11)*
☐ *IRAP [Australie]*	☐ *PIPEDA [Canada]*	☐ *ICREA*
☐ *MTCS de niveau 3 [Singapour]*	☐ *Loi sur la protection des données [Australie]*	☐ *IT Grundschutz [Allemagne]*
☐ *PCI DSS niveau 1*	☐ *Loi sur la protection des données [Nouvelle-Zélande]*	☐ *MARS – E*
☐ *Règle SEC 17-a-4(f)*	☐ *Autorisation DPA - Espagne*	☐ *MITA 3.0*
☐ *SOC1 / ISAE 3402*	☐ *Royaume-Uni DPA - 1988*	☐ *MPAA*
☐ *SOC2 / SOC3*	☐ *VPAT/Section 508*	☐ *NIST*
		☐ *Niveaux Uptime Institute*
		☐ *Principes de sécurité du cloud - Royaume-Uni*

L'utilisation des rapports de conformité ci-dessus permet aux organisations du secteur public d'évaluer des offres uniques concernant les normes de sécurité, de conformité et opérationnelles acceptées. Ces rapports peuvent démontrer que le CISP, en s'y conformant, répond aux contrôles d'opération de Datacenter ci-dessous, requis auprès du fournisseur de service de cloud public. L'exigence de conformité à ces rapports permet aux entités du secteur public de s'assurer que les contrôles ci-dessous sont en place.

- ***Accès surveillé :*** *le CISP doit limiter l'accès physique aux personnes qui ont besoin de se trouver dans un lieu donné pour une raison professionnelle justifiée. Si l'accès est accordé, il doit être retiré dès que le travail nécessaire a été effectué.*
- ***Entrée contrôlée et surveillée :*** *l'entrée dans la couche du Datacenter du périmètre doit être contrôlée. Le CISP doit placer des agents de sécurité aux portes d'entrée et employer des superviseurs qui contrôlent les agents et les visiteurs grâce à*

des caméras de sécurité. Lorsque des personnes autorisées se trouvent sur site, elles doivent recevoir un badge qui requiert une authentification multifacteur et limite l'accès aux zones préapprouvées.

- ***Employés du Datacenter du CISP :*** *les employés CISP qui accèdent régulièrement à un Datacenter doivent recevoir des autorisations d'accès aux zones concernées du site selon leur poste, et l'accès doit être régulièrement contrôlé. Les registres de personnel doivent être révisés régulièrement par un responsable d'accès à la zone, afin de s'assurer que l'autorisation de chaque employé est toujours nécessaire. Si un employé n'a pas besoin actuellement de se trouver dans un Datacenter, il doit passer par le processus réservé aux visiteurs.*

- ***Surveillance d'une entrée non autorisée :*** *les CISP doivent continuellement surveiller les entrées non autorisées sur la propriété du Datacenter, en utilisant la vidéosurveillance, la détection des intrusions et l'accès aux journaux des systèmes de surveillance. Les entrées doivent être sécurisées par des appareils qui déclenchent une alarme si une porte est forcée ou maintenue ouverte.*

- ***Sécurité globale des moniteurs de centres des opérations de sécurité du CISP :*** *les centres d'opérations de sécurité du CISP doivent se trouver dans le monde entier et être responsables de la surveillance, de la répartition et de l'exécution de programmes de sécurité pour les Datacenters du CISP. Ils doivent superviser la gestion des accès physiques et la réponse à la détection des intrusions, tout en fournissant un support international 24 h/24, 7 j/7 aux équipes de sécurité du Datacenter sur site en fournissant des activités de surveillance continues, comme le suivi des activités d'accès, la révocation des autorisations d'accès et la disponibilité pour répondre à et analyser un incident de sécurité potentiel.*

- ***Vérification des accès couche par couche :*** *l'accès à la couche d'infrastructure doit être restreint en fonction du besoin professionnel. En mettant en place une vérification des accès couche par couche, le droit d'entrer dans chaque couche n'est pas accordé par défaut. L'accès à une couche spécifique ne doit être accordé que si nécessaire.*

- ***Le maintien de l'équipement fait partie des opérations régulières :*** *les équipes CISP doivent exécuter des diagnostics sur les machines, les réseaux et l'équipement de sauvegarde en cas d'urgence ou afin de s'assurer qu'il fonctionne correctement. Les contrôles de maintenance de routine sur l'équipement et les installations du Datacenter doivent faire partie des opérations régulières du Datacenter du CISP.*

- ***Équipement de secours en cas d'urgence :*** *l'eau, l'électricité, les télécommunications et la connexion Internet doivent être conçues de manière redondante, afin que le CISP puisse maintenir un fonctionnement continu même en cas d'urgence. Les systèmes d'alimentation électrique doivent être conçus pour être entièrement redondants, afin que, même en cas d'interruption, des unités d'alimentation non interruptibles puissent être utilisées pour certaines fonctions. Des générateurs peuvent apporter une alimentation de secours à toutes les installations. Les personnes et systèmes doivent surveiller et contrôler la température et l'humidité pour éviter toute surchauffe, ce qui réduit encore davantage les éventuelles pannes de service.*

- ***La technologie et les personnes travaillent ensemble pour plus de sécurité :*** *des procédures obligatoires doivent être en place pour obtenir l'autorisation d'entrer dans la couche de données. Des personnes autorisées doivent ainsi vérifier et approuver les demandes d'accès. Dans le même temps, des systèmes de détection des menaces et des intrusions électroniques doivent surveiller et déclencher automatiquement des alertes de menaces identifiées ou d'activité suspecte. Par exemple, si une porte est maintenue ouverte ou forcée, une alarme se déclenche. Le CISP doit déployer des caméras de sécurité et conserver les enregistrements conformément aux exigences légales et réglementaires.*

- ***Empêcher toute intrusion physique et technologique :*** *les points d'accès aux salles de serveurs doivent être fortifiés avec des appareils de contrôle électronique qui requièrent une autorisation multifacteurs. Le CISP doit également être préparé à empêcher toute intrusion technologique. Les serveurs CISP doivent pouvoir avertir les employés de toute tentative de suppression des données. Dans le cas improbable d'une violation, le serveur doit être automatiquement désactivé.*

- ***Les serveurs et supports reçoivent une attention rigoureuse :*** *les appareils de stockage de support utilisés pour stocker les données du client doivent être classés par le CISP en tant que Critiques et, par conséquent, être traités en tant qu'appareils à risque élevé, tout au long de leur cycle de vie. Le CISP doit avoir des normes rigoureuses sur la manière d'installer, d'entretenir et éventuellement de détruire les appareils lorsqu'ils ne sont plus utilisés. Lorsqu'un appareil de stockage a atteint la fin de sa durée de vie utile, le CISP met le support hors service en utilisant les techniques détaillées dans la norme NIST 800-88. Les supports qui accueillaient des données du client continuent d'être contrôlés par le CISP jusqu'à ce qu'ils aient été mis hors service en toute sécurité.*

- ***Les auditeurs tiers vérifient les procédures et systèmes CISP :*** *le CISP doit être audité par des auditeurs externes pour inspecter les Datacenters, en effectuant un contrôle approfondi pour vérifier que le CISP respecte les règles établies*

nécessaires à l'obtention de ses certifications de sécurité. Selon le programme de conformité et ses exigences, les auditeurs externes peuvent s'entretenir avec les employés du CISP concernant la manière dont ils gèrent les supports et les mettent hors service. Les auditeurs peuvent également surveiller les entrées et couloirs d'un Datacenter grâce aux caméras de sécurité. Ils peuvent aussi examiner l'équipement, comme les appareils de contrôle d'accès électronique CISP et les caméras de sécurité.

- ***Prêt à faire face à l'inattendu :*** *le CISP doit se préparer de façon proactive à faire face aux menaces environnementales potentielles, comme les catastrophes naturelles et les incendies. Le CISP peut protéger les Datacenters en installant des capteurs automatiques et un équipement réactif, par exemple. Des appareils de détection de l'eau doivent être installés pour alerter les employés de problèmes ; les pompes automatiques retirent le liquide et évitent tout dommage. De même, les équipements automatiques de détection et de suppression des incendies réduisent les risques et peuvent avertir les employés du CISP et les pompiers en cas de problème.*

- ***Disponibilité élevée dans plusieurs zones de disponibilité :*** *le CISP doit fournir plusieurs zones de disponibilité pour une tolérance aux pannes supérieure. Chaque zone de disponibilité doit se composer d'un ou plusieurs Datacenters, être physiquement séparée des autres et avoir une alimentation et une mise en réseau redondantes. Les zones de disponibilité doivent être reliées les unes aux autres avec une mise en réseau à fibre optique rapide et privée, afin de concevoir des applications qui basculent automatiquement entre les zones de disponibilité sans interruption.*

- ***Simulation d'interruptions et mesure de notre réponse*** *: le CISP doit avoir un plan de continuité des opérations en tant que guide de traitement des opérations, expliquant comment éviter et réduire les interruptions dues aux catastrophes naturelles, avec des étapes détaillées à suivre avant, pendant et après un événement. Pour limiter l'inattendu et s'y préparer, le CISP doit tester régulièrement le plan de continuité des opérations avec des exercices qui simulent différents scénarios. Le CISP doit documenter les performances de ses employés et processus, puis livrer un compte-rendu des enseignements qui en sont tirés et des actions correctives qui peuvent être nécessaires pour améliorer le taux de réponse. L'équipe du CISP doit être formée et prête à réagir rapidement après les interruptions, grâce à un processus de récupération méthodique qui minimise davantage le temps d'interruption dû à des erreurs.*

- ***Aider à atteindre les objectifs d'efficacité :*** *en plus de traiter les risques pour l'environnement, le CISP doit également intégrer des considérations en matière de développement durable dans la conception du Datacenter. Le CISP doit fournir des détails sur son engagement à utiliser une énergie renouvelable pour ses Datacenters, et fournir des informations sur la manière dont ses clients peuvent réduire les émissions carbone par rapport à ses propres Datacenters.*

- ***Sélection de site*** *: avant de choisir une localisation, le CISP doit effectuer des évaluations initiales en matière d'environnement et de zone géographique. Les localisations des Datacenters doivent être soigneusement sélectionnés de manière à limiter les risques environnementaux, comme les inondations, les conditions climatiques extrêmes et l'activité sismique. Les zones de disponibilité du CISP doivent être conçues de manière indépendante et physiquement séparées les unes des autres.*

- ***Redondance :*** *les Datacenters doivent être conçus pour anticiper et tolérer les défaillances tout en maintenant les niveaux de service. En cas de défaillance, les processus automatisés doivent éloigner le trafic de la zone affectée. Les applications essentielles doivent être déployées selon une norme N+1 de manière à ce que, en cas de défaillance d'un Datacenter, la capacité soit suffisante pour permettre un équilibrage de charge du trafic vers les autres sites.*

- ***Disponibilité :*** *le CISP doit identifier les composants essentiels des systèmes nécessaires pour assurer la disponibilité de son système, et récupérer le service en cas de panne. Les composants système essentiels doivent être sauvegardés dans plusieurs endroits isolés. Chaque localisation ou zone de disponibilité doit être conçu(e) de manière à fonctionner indépendamment avec une haute fiabilité. Les zones de disponibilité doivent être connectées pour permettre aux applications de basculer automatiquement entre les zones de disponibilité sans interruption. Des systèmes hautement résilients, et donc la disponibilité du service, doivent être fonction de la conception du système. La conception du Datacenter en termes de zones de disponibilité et de réplication des données doivent permettre aux clients du CISP d'atteindre des objectifs de temps et de point de récupération extrêmement courts, de même que les plus hauts niveaux de disponibilité.*

- ***Planification de la capacité*** *: le CISP doit continuellement surveiller l'utilisation du service pour déployer l'infrastructure afin de soutenir les engagements et exigences en termes de disponibilité. Le CISP doit maintenir un modèle de planification de la capacité qui évalue l'utilisation et les demandes de l'infrastructure CISP au moins une fois par mois. Ce modèle doit soutenir la planification des futures demandes et comprendre des considérations comme le traitement d'informations, les télécommunications et le stockage de journal d'audit.*

CONTINUITÉ DES OPÉRATIONS et REPRISE APRÈS SINISTRE

- ***Plan de continuité des opérations :*** *le plan de continuité des opérations du CISP doit exposer les mesures permettant d'éviter et de diminuer les interruptions environnementales. Il doit inclure des détails opérationnels sur les étapes à suivre avant, pendant et après un événement. Le plan de continuité des opérations doit être soutenu par des tests comprenant des simulations de différents scénarios. Pendant et après les tests, le CISP doit documenter les performances des personnes et des processus, les actions correctives et les enseignements qui en sont tirés en vue d'une amélioration continue.*

- ***Réponse pandémique :*** *le CISP doit intégrer des politiques et procédures de réponse pandémique dans sa planification de reprise après sinistre, afin de se préparer à répondre rapidement aux menaces infectieuses. Les stratégies d'atténuation comprennent des modèles de personnel alternatif pour transférer les processus essentiels vers des ressources extérieures à la région, et l'activation d'un plan de gestion des crises pour soutenir les opérations professionnelles critiques. Les plans pandémiques doivent faire référence aux agences et réglementations de santé internationales, y compris les contacts au sein des agences internationales.*

SUPERVISION ET JOURNALISATION

- ***Vérification de l'accès au Datacenter :*** *l'accès aux Datacenters doit être régulièrement contrôlé. L'accès doit être automatiquement révoqué lorsque le dossier d'un employé est clôturé dans le système de RH du CISP. De plus, lorsque l'accès d'un employé ou sous-traitant expire en accord avec la durée de la requête approuvée, son accès doit être révoqué, même s'il reste un employé du CISP.*

- ***Journaux d'accès au Datacenter*** *: l'accès physique aux Datacenters du CISP doit être consigné, surveillé et conservé. Le CISP doit mettre en corrélation les informations tirées des systèmes de surveillance logiques et physiques pour améliorer la sécurité selon le besoin.*

- ***Surveillance de l'accès au Datacenter :*** *le CISP doit surveiller les Datacenters en utilisant des centres d'opérations de sécurité internationaux, qui surveillent, trient et exécutent les programmes de sécurité. Ils doivent fournir un support international 24 h/24, 7 j/7 en gérant et en surveillant les activités d'accès au Datacenter, en équipant les équipes locales et autres équipes de support pour qu'elles réagissent aux incidents de sécurité en triant, consultant, analysant et en distribuant les réponses.*

SURVEILLANCE et DÉTECTION

- ***Vidéosurveillance :*** *les points d'accès physique aux salles de serveurs doivent être enregistrés par un système de vidéosurveillance en circuit fermé. Les images doivent être conservées conformément aux exigences juridiques et de conformité.*

- ***Points d'entrée du Datacenter :*** *l'accès physique doit être contrôlé aux points d'accès du bâtiment par des professionnels de la sécurité utilisant la surveillance, des systèmes de détection d'intrusion et autres moyens électroniques. Le personnel autorisé doit utiliser des mécanismes d'authentification multifacteur pour accéder aux Datacenters. Les entrées dans les salles de serveurs doivent être sécurisées avec des appareils émettant des alarmes pour lancer une réponse aux incidents si la porte est forcée ou maintenue ouverte.*

- ***Détection des intrusions :*** *les systèmes de détection des intrusions électroniques doivent être installés dans la couche de données pour surveiller, détecter et alerter automatiquement le personnel approprié en cas d'incidents de sécurité. Les points d'entrée et de sortie dans les salles de serveurs doivent être sécurisés avec des appareils qui requièrent que chaque personne fournisse une authentification multifacteur avant d'autoriser l'entrée ou la sortie. Ces appareils déclenchent des alarmes si l'ouverture de la porte est forcée sans authentification ou si la porte est maintenue ouverte. Des alarmes de porte doivent également être configurées pour détecter les cas dans lesquels une personne sort d'une couche de données ou y entre sans fournir d'authentification multifacteur. Les alarmes doivent être immédiatement envoyées à des centres d'opérations de sécurité du CISP 24 h/24, 7 j/7 pour consignation, analyse et réponse immédiates.*

GESTION DES APPAREILS

- ***Gestion des actifs :*** *les actifs CISP doivent être gérés de manière centralisée grâce à un système de gestion de l'inventaire qui stocke et suit le propriétaire, la localisation, l'état, la maintenance et les informations descriptives pour les actifs*

appartenant au CISP. Suite à l'approvisionnement, les actifs doivent être scannés et suivis, et les actifs subissant une maintenance doivent être vérifiés et surveillés concernant l'appartenance, le statut et la résolution.

- ***Destruction des supports :*** *les appareils de stockage de support utilisés pour stocker les données du client doivent être classés par le CISP en tant que Critiques et traités en conséquence, en tant qu'appareils à impact élevé, tout au long de leur cycle de vie. Le CISP doit avoir des normes rigoureuses sur la manière d'installer, d'entretenir et éventuellement de détruire les appareils lorsqu'ils ne sont plus utilisés. Lorsqu'un appareil de stockage a atteint la fin de sa durée de vie utile, le CISP doit mettre le support hors service en utilisant les techniques détaillées dans la norme NIST 800-88. Les supports qui accueillaient des données du client continuent d'être contrôlés par le CISP jusqu'à ce qu'ils aient été mis hors service en toute sécurité.*

SYSTÈMES DE SUPPORT OPÉRATIONNEL

- ***Alimentation :*** *les systèmes d'alimentation électrique des Datacenters du CISP doivent être conçus pour être totalement redondants et maintenables sans que cela ait une quelconque incidence sur les opérations, 24 h/24. Le CISP doit veiller à ce que les Datacenters soient équipés d'une alimentation de secours, afin de garantir qu'une alimentation soit disponible pour maintenir les opérations en cas de panne électrique pour des charges critiques et essentielles dans les installations.*

- ***Climat et température :*** *les Datacenters du CISP doivent utiliser des mécanismes pour contrôler le climat et maintenir une température de fonctionnement appropriée pour les serveurs et autres matériels, afin d'éviter la surchauffe et de réduire la possibilité de pannes de service. La température et l'humidité doivent être surveillées et régulées aux niveaux appropriés par le personnel et par divers systèmes.*

- ***Détection et suppression des incendies*** *: les Datacenters CISP doivent être dotés d'un équipement automatique de détection et de suppression des incendies. Les systèmes de détection des incendies doivent utiliser des capteurs de détection de la fumée dans les espaces de mise en réseau, mécaniques et d'infrastructure. Ces zones doivent également être protégées par des systèmes de suppression.*

- ***Détection des fuites :*** *le CISP doit équiper les Datacenters de fonctionnalités de détection des fuites d'eau. Si de l'eau est détectée, des mécanismes permettant d'évacuer l'eau doivent être en place afin d'éviter tout dommage supplémentaire lié à l'eau.*

MAINTENANCE DE L'INFRASTRUCTURE

- ***Maintenance de l'équipement*** *: le CISP doit surveiller et effectuer une maintenance préventive de l'équipement électrique et mécanique pour maintenir la continuité du fonctionnement des systèmes dans les Datacenters CISP. Les procédures de maintenance de l'équipement doivent être effectuées par des personnes qualifiées selon un calendrier de maintenance documenté.*

- ***Gestion de l'environnement :*** *le CISP doit surveiller les systèmes et équipements électriques et mécaniques afin de permettre l'identification immédiate des problèmes. Cette supervision doit être effectuée grâce à des outils et informations d'audit continus, fournis via des systèmes de gestion des bâtiments et de supervision électronique du CISP. Une maintenance préventive doit être réalisée afin de s'assurer du fonctionnement continu de l'équipement.*

GOUVERNANCE ET RISQUE

- ***Gestion des risques en cours du Datacenter :*** *le centre des opérations de sécurité du CISP doit évaluer régulièrement les menaces et vulnérabilités des Datacenters. L'évaluation et la limitation en cours des vulnérabilités potentielles doivent être effectuées grâce à des activités d'évaluation des risques du Datacenter. Cette évaluation doit être effectuée en plus du processus d'évaluation des risques au niveau de l'entreprise, utilisé pour identifier et gérer les risques auxquels l'entreprise fait face dans son ensemble. Ce processus doit également prendre en compte les risques réglementaires et environnementaux de la région.*

- ***Attestation de sécurité tierce :*** *des tests tiers des Datacenters du CISP, comme indiqué dans ses rapports de tiers, doivent veiller à ce que le CISP ait correctement mis en œuvre les mesures de sécurité en lien avec les règles établies nécessaires à l'obtention des certifications de sécurité. Selon le programme de conformité et ses exigences, des auditeurs externes peuvent tester la mise hors service des supports, visionner les vidéos des caméras de sécurité, observer les entrées et allées et couloirs dans un Datacenter, tester les appareils électroniques de contrôle de l'accès et examiner l'équipement du Datacenter.*

7. Migrations

	Exigence
1.	***SERVICE DE MIGRATION :*** *Combien de services de migration de données différents le fournisseur de cloud offre-t-il ?*
2.	***MIGRATIONS – SUPERVISION CENTRALISÉE :*** *Le fournisseur de cloud offre-t-il aux organisations un service centralisé c.-à-d. à partir d'un seul écran), avec lequel elles peuvent suivre et surveiller le statut de leur serveur et les migrations d'application ?*
3.	***MIGRATIONS – TABLEAU DE BORD :*** *L'outil de migration du fournisseur de cloud offre-t-il un tableau de bord permettant de visualiser rapidement le statut de migration, les métriques associées ainsi que l'historique de la migration ?*
4.	***MIGRATIONS – OUTILS DU FOURNISSEUR DE CLOUD :*** *L'outil de migration du fournisseur de cloud permet-il l'intégration aux autres outils de migration du fournisseur de cloud qui effectuent des migrations de serveur et d'applications ?*
5.	***MIGRATIONS – OUTILS TIERS :*** *L'outil de migration du fournisseur de cloud permet-il d'intégrer des outils de migration tiers ?* • *Si oui, quels sont les outils de migration tiers pris en charge ?*
6.	***MIGRATIONS – MIGRATIONS SUR PLUSIEURS RÉGIONS :*** *L'outil de migration du fournisseur de cloud offre-t-il la fonctionnalité de suivi et de supervision pour les migrations de serveur et d'application survenant dans des régions différentes ?*
7.	***MIGRATIONS – MIGRATION DU SERVEUR :*** *L'outil de migration du fournisseur de cloud offre-t-il un moyen de migrer des serveurs virtualisés sur site vers le cloud ?* • *Si oui, quels sont les environnements virtualisés actuellement pris en charge ?*
8.	***MIGRATIONS – DÉCOUVERTE DU SERVEUR :*** *L'outil de migration du fournisseur de cloud possède-t-il la fonctionnalité de détection permettant de trouver automatiquement les serveurs virtuels sur site qu'il faut migrer sur le cloud ?*
9.	***MIGRATIONS – DONNÉES DE PERFORMANCES DU SERVEUR :*** *L'outil de migration du fournisseur de cloud permet-il de collecter et d'afficher les performances du serveur et/ou de la machine virtuelle telles que l'utilisation de l'unité de traitement central virtuelle (CPU) et de la mémoire vive disponible (RAM) ?*
10.	***MIGRATIONS – BASE DE DONNÉES DE DÉCOUVERTE :*** *L'outil de migration du fournisseur de cloud est-il en mesure de stocker toutes les données collectées dans une base de données centralisée ?* • *Si oui, les organisations ont-elles la possibilité d'exporter ces données ? Dans quels formats ?*
11.	***MIGRATIONS – CHIFFREMENT DES DONNÉES INACTIVES :*** *Le fournisseur de cloud chiffre-t-il toutes les informations recueillies et stockées dans la base de données de recherche ?*
12.	***MIGRATIONS – RÉPLICATION INCRÉMENTIELLE DE SERVEUR :*** *L'outil de migration du fournisseur de cloud offre-t-il une réplication de serveur incrémentielle automatisée et en direct lors de la migration du serveur ou de la machine virtuelle, comme moyen de garantir que toutes les modifications apportées au serveur ou à la machine virtuelle figurent dans l'image finale migrée ?*

	• *Si oui, pendant combien de temps ce service peut-il s'exécuter ?*
13.	*MIGRATIONS – VMWARE :* *L'outil de migration du fournisseur de cloud prend-il en charge les migrations de machines virtuelles VMWare depuis les sites vers le cloud ?*
14.	*MIGRATIONS – HYPER-V :* *L'outil de migration du fournisseur de cloud prend-il en charge les migrations de machines virtuelles Hyper-V depuis les sites vers le cloud ?*
15.	*MIGRATIONS – DÉCOUVERTE D'APPLICATION :* *L'outil de migration du fournisseur de cloud est-il en mesure de détecter et de regrouper les applications avant leur migration ?*
16.	*MIGRATIONS – MAPPAGE DE DÉPENDANCE :* *L'outil de migration du fournisseur de cloud est-il en mesure de détecter les dépendances entre serveurs et applications avant leur migration ?*
17.	*MIGRATIONS – MIGRATION DE BASE DE DONNÉES :* *L'outil de migration du fournisseur de cloud offre-t-il la possibilité de migrer des bases de données sur site vers le cloud ?*
18.	*MIGRATIONS – TEMPS D'ARRÊT DE MIGRATION DE BASE DE DONNÉES :* *L'outil de migration du fournisseur de cloud a-t-il la possibilité d'effectuer une migration de base de données vers le cloud avec un temps d'arrêt minimum, c'est-à-dire que la base de données source devrait rester pleinement opérationnelle pendant le processus de migration ?*
19.	*MIGRATIONS – BASE DE DONNÉES SOURCE :* *L'outil de migration du fournisseur de cloud prend-il en charge la migration de différentes sources de bases de données comme Oracle, SQL Server, etc. ?* • *Si oui, veuillez énumérer toutes les bases de données source qui peuvent être migrées vers le cloud.*
20.	*MIGRATIONS – MIGRATIONS HÉTÉROGÈNES :* *L'outil de migration du fournisseur de cloud a-t-il la possibilité d'effectuer des migrations hétérogènes de bases de données, à savoir, depuis une base de données source vers des bases de données cibles différentes, comme depuis Oracle vers SQL Server ?* • *Si oui, veuillez citer toutes les combinaisons possibles de migrations hétérogènes de bases de données.*
21.	*MIGRATIONS – MIGRATION DE DONNÉES DE PLUSIEURS PÉTAOCTETS :* *Le fournisseur de cloud offre-t-il une solution de transport de données de plusieurs pétaoctets qui utilise des composants sécurisés pour transférer des volumes importants de données depuis et vers le cloud ?*
22.	*MIGRATIONS – MIGRATION DE DONNÉES DE PLUSIEURS EXAOCTETS :* *Le fournisseur de cloud offre-t-il une solution de transport de données de plusieurs exaoctets pour déplacer des volumes de données extrêmement importants vers le cloud ?*
23.	*MIGRATIONS – SAUVEGARDES D'ENTREPRISE :* *Le fournisseur de cloud offre-t-il un service pour intégrer de façon transparente un Datacenter de client à des services de stockage dans le cloud qui permettent de transférer et de stocker des données dans le service de stockage du fournisseur de cloud ?*
24.	*MIGRATIONS – SAUVEGARDES D'ENTREPRISE – STOCKAGE D'OBJET :* *Le service de sauvegardes d'entreprise du fournisseur de cloud offre-t-il l'intégration au service de stockage d'objets dans le cloud du fournisseur ?*

25.	***MIGRATIONS – SAUVEGARDES D'ENTREPRISE – ACCÈS AU FICHIER :*** *Le service de sauvegardes d'entreprise du fournisseur de cloud permet-il aux utilisateurs de stocker et d'extraire des objets en utilisant des protocoles de fichiers comme le protocole NFS (Network File System) ?*
26.	***MIGRATIONS – SAUVEGARDES D'ENTREPRISE – ACCÈS AU BLOC :*** *Le service de sauvegardes d'entreprise du fournisseur de cloud permet-il aux utilisateurs de stocker et d'extraire des objets en utilisant des protocoles de bloc comme le protocole iSCSI (Internet Small Computer Systems Interface) ?*
27.	***MIGRATIONS – SAUVEGARDES D'ENTREPRISE – ACCÈS À LA BANDE :*** *Le service de sauvegardes d'entreprise du fournisseur de cloud permet-il aux utilisateurs de sauvegarder leurs données sur une bibliothèque de bandes virtuelles et de stocker ces sauvegardes de bande sur le cloud du fournisseur ?*
28.	***MIGRATIONS – SAUVEGARDES D'ENTREPRISE – CHIFFREMENT :*** *Le service de sauvegardes d'entreprise du fournisseur de cloud permet-il le chiffrement des données au repos et en transit ?*
29.	***MIGRATIONS – SAUVEGARDES D'ENTREPRISE – INTÉGRATION DE LOGICIEL TIERS :*** *Le service de sauvegardes d'entreprise du fournisseur de cloud s'intègre-t-il aux logiciels de sauvegarde tiers couramment utilisés ?*
30.	***MIGRATIONS – LIMITES DE SERVICE :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des limites de service) concernant la section de migrations ci-dessus ?* *Exemple :* *Nombre maximal de migrations de machines virtuelles simultanées.* *Nombre maximal de solutions de transport de données à commander*

8. Facturation

	Exigence
1.	***FACTURATION – SUIVI ET CRÉATION DE RAPPORTS :*** *Le fournisseur de cloud offre-t-il un service de suivi et création de rapports pour la facturation afin d'aider les utilisateurs à gérer et surveiller leur utilisation des offres cloud ?*
2.	***FACTURATION – ALARMES ET NOTIFICATIONS :*** *Le fournisseur de cloud offre-t-il aux utilisateurs un mécanisme pour configurer des alarmes avec des notifications pour alerter les utilisateurs lorsque leurs dépenses ont dépassé un seuil spécifique ?*
3.	***FACTURATION – GESTION DES COÛTS :*** *Le fournisseur de cloud offre-t-il un mécanisme permettant de générer et d'afficher des graphiques qui récapitulent les coûts et les dépenses ?*
4.	***FACTURATION – BUDGETS :*** *Le fournisseur de cloud offre-t-il un mécanisme permettant d'afficher et gérer les budgets, et de prévoir les coûts estimés ?*
5.	***FACTURATION – VUE CONSOLIDÉE :*** *Le fournisseur de cloud offre-t-il un mécanisme permettant de consolider la facturation de plusieurs comptes sous un compte de règlement principal unique ?*
6.	***FACTURATION – LIMITES DE SERVICE :***

	Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des limites de service) concernant la section de facturation ci-dessus ? *Exemple :* *Nombre maximum de comptes pouvant être regroupés* *Nombre maximal d'alarmes pouvant être créées* *Nombre maximal de budgets pouvant être gérés*

9. Gestion

	Exigence
1.	***GESTION – SERVICE DE SUPERVISION :*** *Le fournisseur de cloud offre-t-il un service de supervision permettant de gérer les applications et les ressources du cloud, qui collecte, surveille et génère des rapports avec des métriques prédéfinies ?*
2.	***GESTION – ALARMES :*** *Le service de supervision du fournisseur de cloud permet-il aux utilisateurs de configurer des alarmes ?*
3.	***GESTION – MÉTRIQUES PERSONNALISÉES :*** *Le service de supervision du fournisseur de cloud permet-il aux utilisateurs de créer et surveiller des métriques personnalisées ?*
4.	***GESTION – GRANULARITÉ DE LA SUPERVISION :*** *Le service de supervision du fournisseur de cloud offre-t-il différents niveaux de supervision, pouvant descendre jusqu'à 1 minute ?*
5.	***GESTION – SERVICE DE SUIVI D'API :*** *Le fournisseur de cloud offre-t-il un service qui journalise, surveille et stocke l'activité sur les ressources cloud au niveau de la console et de l'API (interface de programmation d'application) pour une visibilité améliorée ?* • *Si oui, quels sont les services du fournisseur de cloud qui s'intègrent à ce service se suivi ?*
6.	***GESTION – NOTIFICATION :*** *Le fournisseur du cloud offre-t-il la possibilité d'envoyer des notifications en fonction de niveaux activité d'API (interface de programmation d'application) ?*
7.	***GESTION – COMPRESSION :*** *Le fournisseur de cloud offre-t-il un mécanisme permettant de compresser les journaux générés par le système de suivi de l'API (interface de programmation d'application) afin d'aider les utilisateurs à réduire les coûts de stockage associés à ce service ?*
8.	***GESTION – REGROUPEMENT DES RÉGIONS :*** *Le fournisseur du cloud offre-t-il la possibilité d'enregistrer l'activité d'API (interface de programmation d'application) dans toutes les régions et de fournir ces informations de façon regroupée pour plus de facilité ?*
9.	***GESTION – INVENTAIRE DES RESSOURCES :*** *Le fournisseur de cloud offre-t-il un service pour examiner, contrôler et évaluer les configurations de ressources déployées par un utilisateur ?*
10.	***GESTION – MODIFICATIONS DE CONFIGURATIONS :*** *Le fournisseur de cloud enregistre-t-il automatiquement une modification de configuration de ressource quand elle se produit ?*

11.	***GESTION – HISTORIQUE DE CONFIGURATION :*** *Le fournisseur du cloud offre-t-il la possibilité d'examiner la configuration des ressources à un moment donné dans le passé ?*
12.	***GESTION – RÈGLES DE CONFIGURATION :*** *Le fournisseur de cloud fournit-il des conseils et des recommandations pour l'allocation, la configuration et la supervision continue de la conformité ?*
13.	***GESTION – MODÈLES DE RESSOURCES :*** *Le fournisseur de cloud offre-t-il aux utilisateurs la possibilité de créer, d'allouer et de gérer un ensemble de ressources en se basant sur des modèles ?*
14.	***GESTION – RÉPLICATION DES MODÈLES DE RESSOURCES :*** *Le fournisseur de cloud offre-t-il la capacité de répliquer rapidement ces modèles de ressource dans différentes régions pour pouvoir éventuellement les utiliser dans des situations de reprise après sinistre (DR) ?*
15.	***GESTION – CONCEPTEUR DE MODÈLE :*** *Le fournisseur de cloud offre-t-il un outil graphique facile à utiliser avec une fonctionnalité de glisser-déposer qui accélère le processus de création de tels modèles de ressource ?*
16.	***GESTION – CATALOGUE DES SERVICES :*** *Le fournisseur de cloud offre-t-il un service pour créer et gérer un catalogue de services (serveurs, de machines virtuelles, bases de données, etc.) ?*
17.	***GESTION – ACCÈS À LA CONSOLE :*** *Le fournisseur de cloud offre-t-il une interface utilisateur web pour faciliter la gestion et la supervision des services cloud ?*
18.	***GESTION – ACCÈS À L'INTERFACE DE LIGNE DE COMMANDE :*** *Le fournisseur de cloud offre-t-il un outil unifié pour gérer et configurer plusieurs services cloud à partir de l'interface de ligne de commande (CLI), et permettre l'automatisation des tâches de gestion à l'aide de scripts ?*
19.	***GESTION – ACCÈS MOBILE :*** *Le fournisseur de cloud offre-t-il une application sur smartphone pour permettre aux utilisateurs de se connecter au service cloud et de gérer leurs ressources ?* • *Si oui, cette application est-elle disponible pour iOS et Android ?*
20.	***GESTION – BONNES PRATIQUES :*** *Le fournisseur de cloud dispose-t-il d'un service qui aide les utilisateurs à comparer leur utilisation du cloud aux bonnes pratiques ?*
21.	***GESTION – LIMITES DE SERVICE :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des limites de service) concernant la section de gestion ci-dessus ?* *Exemple :* *Nombre maximum de règles de configuration par compte* *Nombre maximal d'alarmes pouvant être créées* *Nombre maximal de journaux pouvant être stockés*

10. Support

	Exigence
1.	***SUPPORT – SERVICE :*** *Le fournisseur de cloud offre-t-il un support à tout moment, 24 heures par jour, 7 jours sur 7 et 365 jours par an, par téléphone, chat et message électronique ?*
2.	***SUPPORT – NIVEAUX DE SUPPORT :*** *Le fournisseur de cloud offre-t-il différents niveaux de support ?*
3.	***SUPPORT – ALLOCATION DE NIVEAU :*** *Le fournisseur de cloud permet-il aux utilisateurs d'attribuer eux-mêmes les ressources/services consommés à différents niveaux de support en fonction d'une classification précise, et en ne les forçant pas à gérer des comptes cloud distincts pour atteindre et recevoir ces différents niveaux de support ?*
4.	***SUPPORT – FORUMS :*** *Le fournisseur de cloud offre-t-il des forums de support publics permettant à ses clients de discuter de leurs problèmes ?*
5.	***SUPPORT – TABLEAU DE BORD DE L'ÉTAT DES SERVICES :*** *Le fournisseur de cloud offre-t-il un tableau de bord de l'état des services qui affiche les toutes dernières informations sur la disponibilité des services dans plusieurs régions ?*
6.	***SUPPORT – TABLEAU DE BORD PERSONNALISÉ :*** *Le fournisseur de cloud offre-t-il un tableau de bord qui affiche une vue personnalisée des performances et de la disponibilité des services sous-jacents aux ressources spécifiques de l'utilisateur ?*
7.	***SUPPORT – HISTORIQUE DU TABLEAU DE BORD :*** *Le fournisseur de cloud offre-t-il un historique de 365 jours du tableau de bord de l'état des services ?*
8.	***SUPPORT – ASSISTANT DU CLOUD :*** *Le fournisseur de cloud offre-t-il un service qui tient lieu de spécialiste du cloud personnalisé et qui aide les utilisateurs à comparer leur utilisation des ressources aux bonnes pratiques ?*
9.	***SUPPORT – TAM :*** *Le fournisseur de cloud offre-t-il un gestionnaire technique de compte (TAM) qui fournit un savoir-faire technique pour toute la gamme de services cloud ?*
10.	***SUPPORT – PRISE EN CHARGE DES APPLICATIONS TIERCES :*** *Le fournisseur du cloud propose-t-il la prise en charge des systèmes d'exploitation courants et composants courants des piles d'applications ?*
11.	***SUPPORT – API PUBLIQUE :*** *Le fournisseur de cloud propose-t-il une API (interface de programmation d'application) qui interagit par programme avec les demandes de support afin de créer, modifier et fermer celles-ci ?*
12.	***SUPPORT – DOCUMENTATION DES SERVICES :*** *Le fournisseur de cloud propose-t-il des documentations techniques de bonne qualité, accessibles publiquement, pour tous ses services, incluant, sans s'y limiter, des guides d'utilisateur, des didacticiels, des questions fréquentes (FAQ) et des notes de mise à jour ?*
13.	***SUPPORT – DOCUMENTATION DE L'INTERFACE DE LIGNE DE COMMANDE :*** *Le fournisseur de cloud propose-t-il une documentation technique de bonne qualité, accessible publiquement, pour son interface de ligne de commande (CLI) ?*
14.	***SUPPORT – ARCHITECTURES DE RÉFÉRENCE :***

	Le fournisseur de cloud offre-t-il un ensemble gratuit de documents d'architecture de référence pour aider ses clients à créer des solutions spécifiques en combinant de nombreux services qu'il propose ?
15.	***SUPPORT – DÉPLOIEMENTS DE RÉFÉRENCE :*** *Le fournisseur de cloud propose-t-il un ensemble gratuit de documents contenant des procédures étape par étape détaillées, testées et validées, incluant les bonnes pratiques pour implémenter des solutions courantes (DevOps, Big Data, entrepôt de données, applications Microsoft, applications SAP, etc.) dans ses offres cloud ?*

Annexe B - Démonstration

Les démonstrations peuvent représenter un moyen efficace de tester les offres de cloud et de choisir la solution la plus adaptée aux besoins de l'organisation. Voici un exemple de script de démonstration pour les technologies cloud.

1. *Démontrer, à un niveau élevé, la console et les offres/ressources publiquement disponibles des CISP :*
    - *Capacités de stockage*
    - *Capacités de serveur / instance*
    - *Capacités et types de base de données*
    - *Mise en réseau*
    - *Outils de gestion et d'analytique*
    - *Sécurité*
    - *Autres capacités*
2. *Décrivez comment vous utilisez vos technologies cloud utilisées dans la démonstration.*
3. *Démontrez comment vous effectuez cette démonstration en temps réel avec l'offre de cloud.*
4. *Comptes :*
    - *Décrivez le système de clé de compte (source et utilisateur) utilisé dans la démonstration.*
    - *Démontrez comment vous gérez et protégez vos clés de compte.*
5. *Démontrez comment vous sélectionnez la localisation physique pour le stockage de votre application/de vos données.*
6. *Démontrez l'échelle de vos offres en définissant des solutions à grande échelle de serveur / instance et de stockage.*
7. *Montrez comment un utilisateur final demande différents services à partir d'offres de cloud. Démontrez :*
    - *Comment les comptes sont établis*
    - *Comment les provisions de sécurité sont activées*
    - *Comment les comptes principaux peuvent être divisés en sous-comptes*
    - *Comment votre Identity and Access Management (IAM) peut séparer l'accès à différentes ressources :*
        - *Comment sécuriser un compte*
        - *Créer des utilisateurs et des groupes*
        - *Ajouter une politique*
        - *Définir des mots de passe*
8. *Démontrez comment les environnements virtuels peuvent être isolés du point de vue de la sécurité et de la mise en réseau :*
    - *Création de sous-réseaux*
    - *Acheminement sur Internet*
9. *Démontrez comment vous pouvez créer un environnement dans deux localisations isolées ou plus.*
    - *Démontrez l'équilibrage de charge entre les environnements.*
10. *Démontrez la capacité à utiliser plusieurs méthodes pour interagir avec les services de cloud computing (par ex., interface de programmation d'application (API), console web, ligne de commande).*
11. *Stockage :*
    - *Décrivez les options de stockage*
    - *Démontrez les types de stockage disponibles (par ex., bloc, objet) et les processus de cycle de vie des données*
    - *Établissez un volume de stockage et démontrez comment les données sont chargées et récupérées*
    - *Créez un volume de stockage XGB avec et sans option de serveur / instance*
    - *Démontrez et validez les autorisations pour accéder à ces volumes.*

12. *Serveur / instance :*
    - *Décrivez les options de serveur / instance : taille et fonctionnalités des ressources de serveur / instance*
    - *Démontrez l'activation et la désactivation d'une ressource de serveur / instance*
    - *Démontrez les propriétés (capacité à lancer X instances simultanément, sélection de réseau, protection contre la résiliation accidentelle, location, etc.)*
    - *Démontrez une option de serveur / instance avec l'équivalent de X cœurs et X Go de RAM*
    - *Démontrez l'évolution des ressources basées sur la charge en exécutant une application*
    - *Démontrez les capacités de scalabilité automatique*
    - *Démontrez comment le serveur / instance peut être arrêté et redémarré ultérieurement*
    - *Démontrez comment une option de serveur / instance peut être revue à la hausse ou à la baisse et assurer le maintien des opérations*
    - *Démontrez comment une option de serveur / instance peut être copiée*
    - *Démontrez comment configurer des groupes de sécurité*
    - *Décrivez les systèmes d'exploitation disponibles dans l'offre CISP*
    - *Démontrez un exemple d'installation de système d'exploitation Linux*
    - *Décrivez vos capacités à fournir des images destinées à des offres de serveur / instance*
    - *Quels formats d'images prenez-vous en charge ?*
    - *Démontrez comment vous pouvez charger et utiliser une image*
    - *Démontrez l'informatique sans serveur*
    - *Démontrez la capacité à lancer un cluster d'instances de calcul avec différentes tarifications en fonction d'un marché cible*
13. *Base de données :*
    - *Décrivez les capacités de votre base de données*
    - *Démontrez les capacités MySQL, MS SQL Server, Oracle et PostgreSQL et MariaDB*
    - *Démontrez les capacités d'entreposage de données*
    - *Démontrez les capacités à sauvegarder ces ressources*
14. *Mise en réseau : démontrez des options de réseau défini par logiciel et des capacités de gestion de réseau*
15. *Gestion et analyse*
    - *Décrivez vos capacités de gestion cloud et d'analytique*
    - *Démontrez les options de supervision*
    - *Démontrez vos capacités avec les cadres Hadoop*
16. *Sécurité : démontrez la sécurité du réseau*
    - *Décrivez votre approche de la sécurité*
    - *Pare-feu*
    - *Groupes de sécurité*
    - *Passerelles*
    - *NACL*
    - *Journaux système*
    - *Chiffrement*
    - *Accréditations de conformité disponibles*
    - *Stockage des clés*
    - *Autres fonctionnalités*
17. *Approvisionnement : démontrez comment vous pouvez créer une collection de ressources liées au cloud et les approvisionner de manière ordonnée et prévisible à l'aide d'un modèle réutilisable*
18. *Logiciel : démontrez vos capacités à fournir un accès aux logiciels fréquemment utilisés*
19. *Démontrez comment vous pouvez effectuer un transfert des données à grande échelle*
20. *Démontrez les options de facturation, notamment :*
    - *Vue récapitulative, vue granulaire, vue par ressources balisées*

- *Prévisions de dépenses/utilisation d'après les dépenses/utilisations actuelles*

21. *Démontrez les capacités de support et de consulting disponibles*
    - *Quelles options de support sont disponibles*
    - *Proposez-vous des vérifications et des conseils sur l'utilisation du service ?*

Démontrez toutes les autres fonctionnalités de l'offre qui la démarquent, selon vous.