Achat de services cloud dans le secteur public

Manuel – Comprend un modèle de demande de propositions pour un accord-cadre sur le cloud computing

Version 2 : février 2022

Avis

Ce document est fourni à titre informatif seulement. Il n'a pas été élaboré conformément aux exigences juridiques relatives aux processus de passation de marchés publics dans une région particulière. Il incombe aux clients du 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 aucune garantie, obligation, condition, ne fournit aucune assurance et n'établit aucun engagement contractuel.

Les exemples de documents et de texte ne doivent pas être interprétés comme des avis ou des conseils juridiques. Les clients du cloud doivent consulter leurs propres conseillers juridiques concernant leurs responsabilités en vertu de la loi applicable dans leur propre pays d'opérations. Le CISPE décline expressément toute garantie ou responsabilité ou tout dommage associé ou découlant des informations fournies dans ce document.

À propos du CISPE

Le CISPE (*Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) est une association sectorielle indépendante à but non lucratif. Nous représentons les fournisseurs de services d'infrastructure de cloud en Europe, travaillant avec le secteur et les décideurs politiques pour fournir des conseils et des formations sur les services cloud et leur rôle dans le secteur, la vie publique et la société en général.

Nous comptons parmi nos membres un nombre croissant de sociétés opérant dans tous les pays de l'UE et dont le siège social est situé 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 du CISPE sur la protection des données. Nous :

- Promouvons les avantages des politiques de passation de marchés publics « cloud first » au sein de l'UE et de ses États membres
- Engageons le secteur des infrastructures de cloud à atteindre la neutralité climatique d'ici 2030
- Promouvons des exigences de sécurité et des normes techniques cohérentes à l'échelle de l'UE
- Soutenons des exigences complètes de confidentialité grâce à un Code de conduite sur la protection des données
- Œuvrons pour que le marché européen de l'infrastructure de cloud reste ouvert, compétitif et libre de toute dépendance
- Empêchons les obligations injustifiées de surveillance des contenus dans le cadre juridique de l'UE

Nos membres fournissent et maintiennent les « composants fonctionnels de l'informatique » essentiels qui permettent aux gouvernements, aux autorités publiques et aux entreprises de créer leurs propres systèmes et de fournir des services essentiels à des milliards de citoyens. À ce titre, nous contribuons à permettre le développement de technologies et de services de pointe intégrant l'intelligence artificielle (IA), les objets connectés, les véhicules autonomes et la 5G, ainsi que la prochaine génération de technologies de connectivité cellulaire.

Code de conduite relatif aux services d'infrastructure de cloud

Le Code de conduite sur la protection des données du CISPE, lancé publiquement en septembre 2016, a précédé l'application du Règlement général sur la protection des données (RGPD) de l'Union européenne. Il s'aligne sur les exigences strictes du RGPD pour permettre aux fournisseurs d'infrastructures de cloud d'opérationnaliser la conformité de la protection des données et offrir un cadre solide pour aider les clients à sélectionner les fournisseurs de cloud et à faire confiance à leurs services le Code de conduite du CISPE a été validé par le Comité européen de protection des données (CEPD) en mai 2021, et approuvé par la CNIL française agissant en tant qu'autorité compétente en juin 2021. https://www.codeofconduct.cloud/

Pacte sur la neutralité climatique des centres de données

Le CISPE s'est engagé auprès de la Commission européenne fin 2019 à élaborer un ensemble de métriques et une initiative d'autorégulation pour garantir la neutralité climatique des centres de données d'ici 2030. Cette initiative a été élaborée en collaboration avec l'Association européenne des centres de données (EUDCA), ainsi qu'avec d'autres associations professionnelles et acteurs du marché des centres de données. Elle sera lancée en janvier 2021 sous le nom de « Pacte pour des centres de données à neutralité climatique ». https://www.climateneutraldatacentre.net/

Initiative pour un logiciel équitable

En collaboration avec le CIGREF, l'association française des CIO, et avec le soutien d'autres associations professionnelles de CIO et de fournisseurs en Europe, le CISPE a défini 10 principes de licence de logiciel équitable pour les clients du cloud, un ensemble de bonnes pratiques pour les entreprises qui se tournent vers le cloud pour la croissance, l'innovation et la flexibilité, et qui mettent au défi leurs fournisseurs de logiciels de garantir des conditions de licence équitable. https://www.fairsoftware.cloud/

GAIA-X

Le CISPE est l'un des vingt-deux membres fondateurs de GAIA-X, l'initiative européenne qui vise à fournir un écosystème numérique ouvert, transparent et sécurisé. En tant que tel, le CISPE s'est engagé dès le départ à respecter la vision et les principes de l'organisation GAIA-X. Son secrétaire général a été réélu en juin 2021 pour siéger au conseil d'administration. Certains des outils référencés dans le manuel, tels que le Code de conduite de la protection des données du CISPE et le Code de conduite IaaS SWIPO, sont utiles pour démontrer la conformité aux principes de GAIA-X. https://www.gaia-x.eu

Le CISPE et le secteur public

Le CISPE contribue au débat sur les politiques publiques européennes et s'efforce d'assurer une meilleure compréhension du rôle, de la contribution et du potentiel du secteur européen des infrastructures de cloud.

Si les modèles d'achat public doivent conditionner le processus d'adoption et d'utilisation du cloud computing, l'acquisition de services cloud diffère de la plupart des acquisitions technologiques traditionnelles connues du secteur public. Les approches d'approvisionnement doivent être repensées : le CISPE encourage les décideurs politiques de l'UE à développer une approche plus ambitieuse tournée vers l'avenir à l'échelle de l'UE, basée sur des initiatives politiques de type « cloud first », afin de contribuer au développement du marché unique des infrastructures de cloud en Europe et de soutenir les objectifs de croissance du marché unique numérique (MUN).

Le but de ce manuel est de fournir des conseils et un support aux autorités publiques pour l'acquisition de services 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://www.codeofconduct.cloud/public-register/

Table des matières

Résumé et objectif de ce manuel

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

Ce document est fourni à titre informatif seulement. Il n'a pas été élaboré conformément aux exigences juridiques concernant les processus de passation 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 concours** lors de l'achat en dehors d'un accord-cadre de cloud. Les sections du manuel sont organisées de la même façon qu'un AO informatique générique. Des exemples d'appels d'offres génériques et de critères de sélection sont accompagnés de commentaires pour mieux comprendre pourquoi un appel d'offres de cloud est différent d'un appel d'offres informatique traditionnel.

Suite à la publication de la stratégie cloud de la Commission européenne orientant la manière dont les institutions et agences européennes moderniseront leur infrastructure informatique grâce à une approche « cloud first », le CISPE a remis le manuel à la Commission européenne en juillet 2019 lors de l'événement « *Comment transformer les administrations grâce à une politique de cloud intelligente* ».

La **version 2** de ce manuel comprend de nouvelles orientations concernant la protection des données (section 2.3.1.1), le changement de fournisseur de services cloud et le transfert données (section 2.3.1.2), les conditions générales des logiciels (section 2.5.2), la durabilité dans le cloud (section 3.6) et une annexe B actualisée intitulée Évaluation technique en direct.

> ***« Services cloud »*** *désigne toutes les technologies de cloud et les services associés auxquels un utilisateur final peut avoir besoin d'accéder. Cela inclut la consultation ou les services professionnels/gérés 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 Logiciel 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 posture de sécurité et une gestion de la conformité améliorées, tout en réalisant des gains d'efficacité et des économies.

Les méthodes d'approvisionnement informatique traditionnelles pour l'achat de matériel, de logiciels et de centres de données ne s'appliquent pas à l'achat de services cloud. Les approches de tarification, de gouvernance des contrats, de conditions générales, de sécurité, d'exigences techniques, d'accords de niveau de service, etc., changent toutes dans un modèle de cloud computing, et l'utilisation des méthodes d'approvisionnement existantes réduit ou élimine les avantages du cloud.

L'un des meilleurs moyens d'acquérir efficacement des services cloud pour le secteur public est un accord-cadre sur le cloud, une attribution multi-organisationnelle d'un menu de clouds à partir duquel les acheteurs éligibles affiliés à l'organisation acheteuse peuvent acquérir les technologies de cloud et les services associés qui répondent à leurs besoins. Véritable vecteur des contrats de cloud, les accords-cadres permettent d'acheter des services cloud de manière efficace et efficiente. Ainsi, les organisations acheteuses et les entités utilisatrices finales peuvent avoir accès à une gamme complète de services cloud et, en fin de compte, bénéficier de tous les avantages du cloud : agilité, économies d'échelle massives, évolutivité pour atteindre une meilleure disponibilité à moindre coût, diversités des fonctionnalités, rythme d'innovation, capacité de mise à l'échelle pour la couverture de nouvelles zones géographiques.

Notez que ce document porte essentiellement sur l'achat de technologies de cloud Infrastructure en tant que service (IaaS) et Plateforme en tant que service (PaaS), fournies par un ***Fournisseur de services d'infrastructure de cloud (CISP)***. Ces technologies de 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 consultation relative au cloud.*

Veuillez noter également que ce document ne couvre pas tous les aspects de la création d'un cadre complet d'approvisionnement de cloud. De nombreux autres documents du secteur et d'analystes couvrent des sujets tels que les bonnes pratiques d'approvisionnement en cloud, la budgétisation pour le cloud, la gouvernance du cloud, etc. Nous vous conseillons vivement de vous reporter à ces conseils et documents lors du développement d'une stratégie d'approvisionnement de cloud globale. Le tableau 1 ci-dessous donne un aperçu du manuel d'AO de services cloud et indique où se trouvent les exemples de texte pour chaque élément d'une demande de services cloud.

Tableau 1 – Sommaire des sections du manuel d'AO de services 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 Présentation d'un AO de services cloud	Exemple générique de texte d'AO couvrant les sections ci-dessous, et commentaire expliquant la logique de la structure d'AO de services cloud et le texte utilisé
2.1 Établissement d'un AO de services 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 des fournisseurs 2.2.3 Établissement de contrat
2.3 Sécurité	2.3.1 Exigences minimales 2.3.1.1 Protection des données 2.3.1.2 Changement de fournisseurs de cloud et portage des données 2.3.2 Comparaison des fournisseurs 2.3.3 Établissement de contrat
2.4 Tarification	2.4.1 Exigences minimales 2.4.2 Comparaison des fournisseurs
2.5 Configuration de l'exécution du contrat/Conditions générales	2.5.1 Conditions générales 2.5.2 Conditions générales relatives aux logiciels 2.5.3 Comment choisir un soumissionnaire par projet 2.5.4. Intégration et départ
3.0 Bonnes pratiques/Leçons apprises	3.1 Gouvernance du cloud 3.2 Budgétisation pour le cloud 3.3 Comprendre le modèle économique du partenaire 3.4 Courtiers de cloud 3.5 Approvisionnement pré-AO/étude de marché 3.6 Développement durable
Annexe A – Exigences techniques pour la comparaison entre les soumissionnaires	Liste d'exigences technologiques cloud génériques pour les contrats exécutoires ou mini concours
Annexe B – Évaluation technique en temps réel	Un exemple de script pour la démonstration d'un produit technologique cloud (démonstrations de cloud dans le cadre d'un contrat exécutoire ou un mini concours)

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

Un accord-cadre sur le cloud bien conçu peut permettre l'achat de services cloud d'une manière qui profite à la fois aux organisations du secteur public participantes et aux fournisseurs de cloud. Les avantages d'un accord-cadre de cloud bien conçu comprennent :

- Nature coopérative :
    - Le regroupement de plusieurs organisations, afin de passer des commandes pour de exigences similaires est synonyme de commodité, d'efficacité, d'économies et de simplification du processus de commande. Il s'agit d'un moyen efficace de regrouper la demande de plusieurs organisations du secteur public pour des technologies communes et des services cloud associés, tels que des solutions de marketplace et des services de conseil.
- Gamme complète de services cloud :
    - Elle peut inclure dans son champ d'application tous les services de conseil/ professionnels/gérés nécessaires pour soutenir et exécuter pleinement la migration vers le cloud et la prise en charge des charges de travail dans le cloud, en plus des technologies de cloud fournies par le CISP, et des services de marketplace.
    - Ces technologies de cloud peuvent être achetées directement auprès d'un CISP ou via un revendeur désigné.
- Gouvernance de contrat :
    - Elle regroupe des organisations/acheteurs hétérogènes autour d'un ensemble commun de conditions générales et une seule attribution de contrat principal, plutôt que des contrats différents pour chaque organisation.
    - Elle est également avantageuse pour les vendeurs, car elle fournit un processus d'acquisition, des conditions générales et un mécanisme de commande normalisés, plutôt que différents pour chaque organisation du secteur public.
    - Elle apporte la flexibilité. La création, l'approbation et l'exécution d'un contrat de cloud efficace dans le cadre des politiques/réglementations gouvernementales existantes nécessitent une expérimentation et la capacité de s'adapter rapidement. Il est beaucoup plus avantageux de créer un accord-cadre qui permet au secteur public et aux fournisseurs de services cloud de travailler tous ensemble pour améliorer le contrat sur le plan contractuel, mécanique et de l'efficacité. Un contrat pluriannuel qui ne fonctionne pas et ne peut pas être ajusté produit une expérience négative pour les utilisateurs finaux du secteur public, les organisations d'approvisionnement et les fournisseurs de services cloud.

- Choix :
    - Il permet aux acheteurs de faire leur choix parmi plusieurs CISP qualifiés et place la barre haut pour tous les services cloud et services associés, comme une marketplace PaaS/SaaS de cloud et les conseils de cloud.
    - Il permet de contrôler le nombre de fournisseurs dans un cadre en s'assurant que la norme de chaque entité soumissionnaire est correctement vérifiée.

Un accord-cadre d'achat de services cloud est plus efficace lorsqu'il inclut des technologies IaaS/PaaS de base fournies par un CISP, ainsi qu'une marketplace PaaS/SaaS, et des services de conseil auxquels les utilisateurs finaux du secteur public peuvent accéder, au besoin, pour les aider à planifier, à effectuer la transition, à utiliser et à maintenir une charge de travail exécutée dans le cloud. Par conséquent, nous recommandons de diviser un AO de services 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 : CONSEIL EN CLOUD
  Services de conseil en cloud (formation, services professionnels, services gérés, etc.) et support technique.

*Comme indiqué précédemment, ce document porte sur l'achat de technologies de 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 distinctes de qualification de fournisseur seront nécessaires pour les fournisseurs des LOT 2 et 3 d'un AO de services cloud.*

La figure 1 ci-dessous donne une vue d'ensemble de la manière dont un appel d'offres de services cloud bien structuré, divisé en trois lots, peut résulter dans un accord-cadre de cloud qui offre aux entités du secteur public une certaine souplesse (tant sur le plan technique que contractuel), une visibilité et un contrôle des dépenses et de l'utilisation du cloud, ainsi que la possibilité de disposer de tous les services cloud nécessaires pour élaborer et maintenir les solutions dont elles ont besoin.

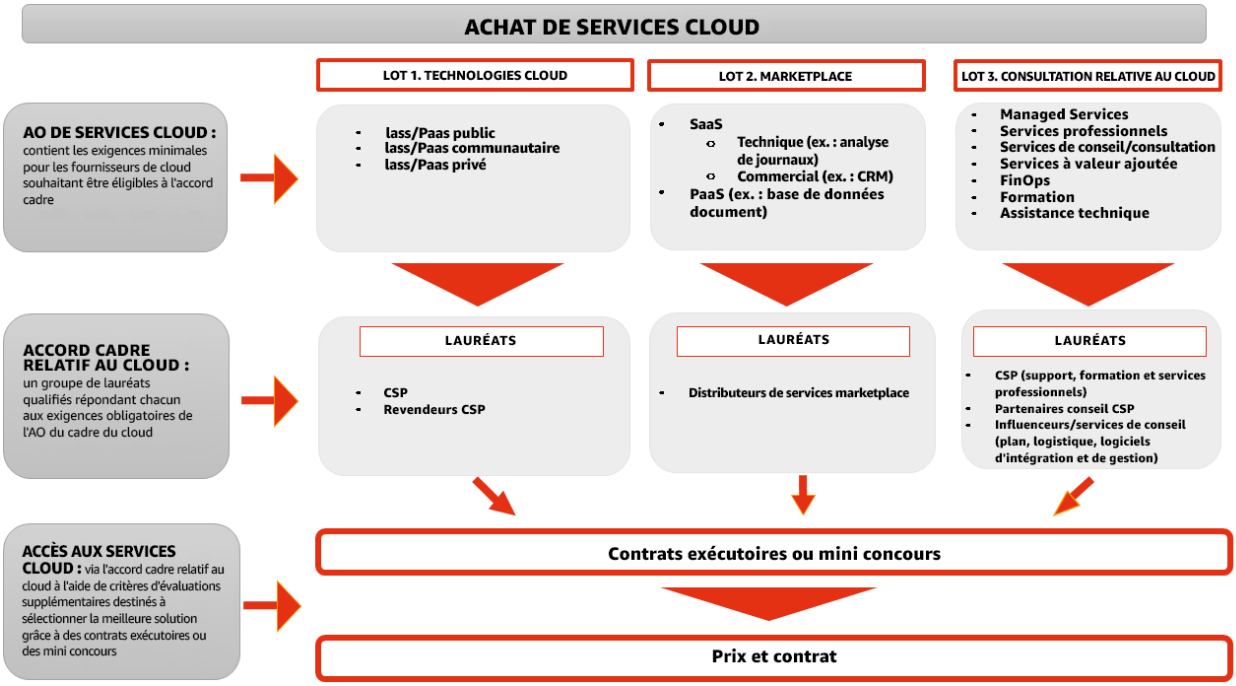

Figure 1 : un AO réussi de services cloud se divise en trois lots. Chaque lot contient des catégories ou des « types d'offres » dans le cadre du lot correspondant, afin de garantir l'adéquation technique et contractuelle avec les exigences de l'utilisateur final lors de l'achat en dehors de l'accord-cadre sur le 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 conseil.

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 de la norme 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 de 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 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 concours ?

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

À la suite de l'appel d'offres et de la mise en place ultérieure de l'accord-cadre sur le cloud, les organismes du secteur public qui sont parties au cadre peuvent commander ou contracter les services cloud dont ils ont besoin lorsque cela est nécessaire. 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 un contrat exécutoire, tout en conservant les avantages de l'accord-cadre.

Si nécessaire, un mini concours peut être organisé, afin d'identifier le meilleur fournisseur pour une charge de travail ou un projet en particulier. Un mini concours est le moment où un client fait appel à la concurrence dans le cadre de l'accord-cadre, en invitant tous les fournisseurs d'un lot à répondre à une série d'exigences. Le client invitera tous les fournisseurs compétents du lot à soumissionner, d'où l'importance des exigences minimales pour les soumissionnaires d'un appel d'offres de services cloud, car elles garantissent un niveau élevé d'options dans chaque lot.

Notez qu'il est important que des ***ensembles distincts de conditions contractuelles*** *existent pour chacun des lots, comme indiqué dans la figure 1 ci-dessus. Une approche unique pour les contrats de tous les LOTS créerait des problèmes de faisabilité technique et de compatibilité.*

2.0 Présentation d'un AO de services cloud

Cette section décrit le modèle et le champ d'application d'un appel d'offres portant sur des services cloud, notamment : les objectifs stratégiques, les participants, les définitions, le calendrier et les exigences administratives minimales. Notez à nouveau que ce manuel porte sur le **LOT 1 : TECHNOLOGIES DE CLOUD**.

2.1 Établissement d'un AO de services cloud

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

2.1.1 Introduction et objectifs stratégiques

Pour atteindre des objectifs stratégiques clairs, il est bon de formuler dans l'introduction d'un AO de services cloud : **(1)** les objectifs commerciaux et les avantages que l'organisation cherche à obtenir en utilisant le cloud, **(2)** la structure de l'accord-cadre : qui achète, qui exploite, qui budgétise, etc., **(3)** une compréhension claire du modèle de responsabilité partagée entre le secteur public et les fournisseurs de services cloud, qui est au cœur de la réussite de l'achat et de l'utilisation du cloud, et **(4)** le type de relation créée entre les fournisseurs de services cloud (CISP), les distributeurs de services de marketplace, les partenaires de conseil, les agences gouvernementales d'achat/d'approvisionnement et les utilisateurs finaux du gouvernement. L'articulation de ces quatre points aide les organisations à développer une demande de propositions qui répond le mieux à leurs besoins, en plus de garantir que les clients et les fournisseurs sont clairs quant aux produits livrables de l'AO.

Un AO de cloud est volontairement différent des AO informatiques traditionnels. La technologie cloud n'est pas simplement un remplacement équivalent des méthodes informatiques traditionnelles ; elle introduit une toute nouvelle façon de consommer la technologie. Les AO de services cloud bien conçus peuvent aider les entités du secteur public à évoluer rapidement pour tirer parti du cloud.

De tous les aspects de l'achat de cloud que nous citons comme une bonne pratique, une compréhension claire du modèle de responsabilité partagée est probablement le meilleur point de départ. Le modèle de responsabilité partagée[1] intervient surtout pour discuter de la sécurité et de la conformité dans le cloud, mais cette délimitation des responsabilités s'applique à tous les aspects des technologies de cloud. Un AO de services cloud doit définir clairement ce qui fait partie des attributions d'un CISP dans un environnement de cloud et ce qui relève de la responsabilité du client. Par exemple, un CISP fournit des fonctionnalités pour contrôler les ressources et les applications qui s'exécutent dans le cloud, ***mais*** il incombe au client d'utiliser effectivement ces fonctionnalités du CISP, car un CISP fonctionnant à grande échelle n'a pas pour vocation de le faire pour des millions de clients.

[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 outre, les clients du cloud doivent comprendre comment le réseau partenaires d'un CISP les aide à utiliser le cloud et à gérer leurs responsabilités. Par exemple, un fournisseur de services managés (MSP) cloud peut aider un client à configurer et à utiliser les fonctionnalités de surveillance fournies par le CISP pour répondre à ses besoins uniques en conformité et audit.

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

Un CISP fournit la technologie de cloud

Un client utilise la technologie de cloud

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

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

Considérez l'achat de services cloud comme un 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 construire une piscine, ou même une maison entière, si vous le souhaitez. Lorsque vous achetez les matériaux et les outils, le personnel peut vous fournir des conseils et une expertise, mais il ne vient pas chez vous pour créer quelque chose pour vous. Plusieurs options s'offrent alors à vous :

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

Si une organisation dispose des compétences internes pour construire et gérer elle-même son environnement et ses solutions de cloud, il lui suffit d'accéder aux technologies et aux outils de cloud standardisés du CISP (directement avec un CISP ou par l'intermédiaire d'un revendeur CISP – voir LOT 1). Les logiciels SaaS et PaaS nécessaires doivent être disponibles sur une marketplace de cloud (LOT 2). Si une aide supplémentaire en conseil, migration, implémentation et/ou gestion est nécessaire, c'est là que le réseau partenaires d'un CISP intervient (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 une facturation à l'utilisation. Les organisations peuvent allouer le type et la taille de ressources dont elles ont besoin pour alimenter leurs nouvelles idées brillantes ou faire fonctionner

leurs services informatiques, sans avoir à investir massivement dans du matériel et/ou des contrats de licence de logiciels à long terme.

*L'**<ORGANISATION>** formule l'exigence de pouvoir accéder à ces types de technologies de cloud commercialement disponibles, afin de pouvoir répondre à ses besoins métier 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 de cloud, ainsi que des services liés au cloud.*

1. ***LOT 1**. Fournisseurs de service cloud (CISP) ou revendeurs CISP pour l'achat de technologies de cloud.*
2. ***LOT 2.** Fournisseurs de services de marketplace.*
3. ***LOT 3.** Fournisseurs de services de conseil pour apporter une 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 :*

- ***Agilité :** mettre les ressources informatiques à la disposition des utilisateurs finaux en quelques minutes au lieu des plusieurs semaines et mois habituels.*
- ***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 exemple CapEx par OpEx). Ne payer que ce qui est consommé.*
- ***Budgétisation :** consulter les informations relatives à la facturation et à l'utilisation, tant au niveau granulaire qu'au niveau récapitulatif, en visualisant les structures de dépenses au fil du temps, ainsi qu'en prédisant les dépenses futures.*
- ***Élasticité :** bénéficier de coûts variables réduits grâce aux 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 centres de données :** se concentrer sur l'activité de nos citoyens et non sur les lourdeurs des racks, des piles et de l'alimentation 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 :** alléger la charge opérationnelle, puisque le CISP exploite, gère et contrôle les composants du système d'exploitation hôte et de la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles le service fonctionne.*
- ***Automatisation :** intégrer l'automatisation dans l'architecture de cloud pour améliorer la capacité de mise à l'échelle en toute sécurité, de manière plus rapide et économique.*
- ***Gouvernance du 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 du 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 à partir de l'infrastructure du CISP, en réduisant la dépendance à l'égard d'un 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 l'emplacement des infrastructures utilisées pour traiter et stocker leurs données (zone urbaine).*
- ***Neutralité climatique :*** *les clients doivent s'engager auprès de CISP qui prennent des mesures spécifiques et éprouvées pour atteindre les objectifs de neutralité climatique d'ici 2030, et qui sont signataires du Pacte pour des centres de données neutres sur le plan climatique. Cela aidera les clients à atteindre leurs propres objectifs de neutralité climatique.*

2.1.2 Calendrier de réponse à l'AO

Une bonne pratique consiste à fournir aux soumissionnaires un calendrier des activités de soumission prévues lors de la création d'un accord-cadre sur le cloud et de l'AO de services 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 du fournisseur s'adaptent au modèle de services cloud.

Notez que le calendrier de l'AO est soumis à la législation locale et aux obligations juridiques. La liste fournie ci-dessous est un guide de bonnes pratiques et non pas 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 cloud :

Calendrier de l'AO de services cloud
• *Publication de la demande d'informations :* • *Réponse à la demande d'informations :* • *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 de l'AO de préqualification :* • *Réponse à l'AO de préqualification :* • *Publication de l'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 à la législation locale et aux obligations juridiques. La liste fournie ci-dessous est un guide de bonnes pratiques et non pas une liste normative d'activités et de délais.

2.1.3 Définitions

Un AO de services cloud doit inclure une liste détaillée de définitions. Cette liste inclut les rôles du fournisseur (par exemple fournisseur de service cloud, revendeur de cloud, partenaire fournisseur), les concepts technologiques généraux (calcul, stockage, IaaS/PaaS, SaaS) et les autres éléments essentiels du contrat. 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 consiste à allouer des ressources de traitement, de stockage, de réseaux et d'autres ressources informatiques fondamentales où le consommateur peut déployer et exécuter des logiciels arbitraires qui peuvent inclure des systèmes d'exploitation et des applications. Le consommateur ne gère ni ne contrôle l'infrastructure de cloud sous-jacente, mais contrôle les systèmes d'exploitation, le stockage et les applications déployées, et éventuellement, dans une certaine mesure, certains composants de réseaux (par exemple, des pare-feu hôtes).*

- ***Plateforme en tant que service (PaaS).*** *La capacité fournie au consommateur consiste à déployer sur l'infrastructure de cloud des applications créées par le consommateur ou acquises par lui, à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure de cloud sous-jacente, notamment le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais il contrôle les applications déployées et éventuellement des paramètres de configuration de l'environnement d'hébergement des applications.*

- ***Logiciel en tant que service (SaaS).*** *Le client a la capacité d'utiliser les applications du fournisseur s'exécutant dans une infrastructure de cloud. Les applications sont accessibles à partir de différents appareils client grâce à une interface client léger, comme un navigateur web (par exemple une messagerie web) ou une interface de programme. Le consommateur ne gère ni ne contrôle l'infrastructure de cloud sous-jacente, notamment le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même les fonctionnalités des applications individuelles, à l'exception peut-être de paramètres de configuration limités propres 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.*

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

- ***Cloud communautaire.*** *L'infrastructure de cloud est allouée pour une utilisation exclusive par une communauté spécifique de consommateurs provenant d'organisations partageant les mêmes intérêts (par exemple, mission, exigences de sécurité, politique et considérations 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 constituée de deux ou plusieurs infrastructures de cloud distinctes (privées, communautaires ou publiques) qui restent des entités uniques, mais qui sont liées entre elles par une technologie standardisée ou propriétaire qui permet la portabilité des données et des applications (par exemple, cloud bursting pour la répartition de charge entre les clouds).*

- ***Cloud privé.*** *L'infrastructure de cloud est allouée pour un usage exclusif par une seule organisation comprenant plusieurs consommateurs (par exemple, 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 d'implémentation et de gestion. Ce point doit être clarifié dans l'AO de services cloud, afin que les fournisseurs de technologies de cloud, les organisations de services de conseil, les grossistes de la marketplace et les entités acheteuses comprennent leurs rôles respectifs.

Concernant le périmètre d'application de l'accord-cadre, et suite à des appels d'offres ou des mini concours, les organisations doivent prendre en considération :

- Qui sera responsable de l'intégration et des services gérés impliquant l'utilisation des technologies de cloud dans le cadre 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 gérés, ou à toute forme de services de main-d'œuvre informatiques ?

Il est important de noter qu'un CISP n'est pas un intégrateur système ni un fournisseur de service managé (MSP). De nombreux clients du secteur public nécessiteront un CISP pour leur IaaS/PaaS, et confieront les tâches de planification, de migration et de gestion à un intégrateur système ou un MSP. La figure 2 ci-dessous décrit les rôles et responsabilités dans un modèle de services cloud.

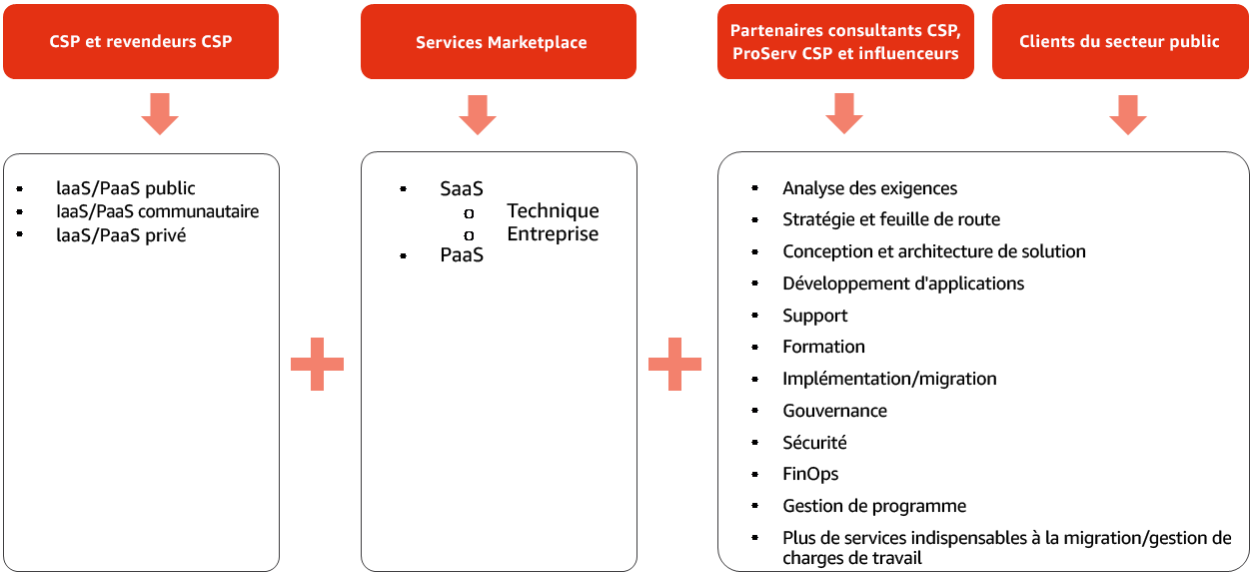

Figure 2 : un AO de services cloud doit fournir aux utilisateurs finaux un menu de tous les services cloud dont ils ont besoin. Les clients du secteur public auront besoin d'un CISP pour les technologies cloud, d'une marketplace pour les produits PaaS et SaaS si besoin. Ainsi, le client pourra déterminer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

L'exemple de texte ci-dessous s'appuie sur les rôles et responsabilités indiqués dans la figure 2 ci-dessus. Un accord-cadre de cloud et l'AO de services 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 la charge de travail/le projet. La meilleure façon de procéder consiste à diviser les services en lots, comme indiqué précédemment, et à déterminer clairement comment sont menés les contrats exécutoires et les mini concours 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 consultation, les services professionnels/l'intégration de système/les services gérés/les services professionnels de migration, 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'approvisionnement tout en optimisant les économies d'échelle.*

Une fois établi, cet accord-cadre permet à une organisation d'acheter les technologies et les services cloud spécifiques qu'elle souhaite, au moment où elle en a besoin, plutôt que 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 est divisé 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 exemple, calcul, stockage, réseaux, base de données, analytique, services d'application, déploiement, gestion, développeur, Internet des objets (IoT), etc.). Comprend des solutions de technologie de 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, BI, la gestion de contenu, l'analyse de journaux, etc.*
3. *LOT 3 : CONSEIL EN CLOUD : portée globale des services de consultation (services gérés, services professionnels, services de conseil/consultation, 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 pour plusieurs lots.

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

CONCURRENCE AU SEIN DU CADRE ET ATTRIBUTION DES CONTRATS

CONTRATS EXÉCUTOIRES

Les organismes du secteur public qui sont parties à l'accord-cadre peuvent commander ou « appeler » les services dont ils ont besoin lorsque cela est nécessaire. 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 un appel, 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, y compris tout engagement précoce sur le marché, les questions de clarification, les courriers électroniques 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 de cadre 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 rechercheront des services.

3. EXAMEN ET ÉVALUATION DES SERVICES

Les acheteurs, en vertu de l'accord-cadre, examineront les descriptions de service 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 de service ou des liens vers les définitions de service*
- *Un document contenant les conditions générales*
- *Un document de tarification (les liens vers la tarification publique 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 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.

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 de fourniture d'une gamme de services*
Caractéristiques non fonctionnelles

MINI CONCOURS

Si nécessaire, un mini concours peut être organisé, afin d'identifier le meilleur fournisseur pour une charge de travail ou un projet en particulier. Un mini concours est le moment où un client fait appel à la concurrence dans le cadre de l'accord-cadre, en invitant tous les fournisseurs d'un lot à répondre à une série 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 centres de données 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 indiquées ci-dessous pour l'offrant.

Notez à nouveau que ce document porte sur le LOT 1 : TECHNOLOGIES CLOUD. Cependant, nous avons ajouté des informations supplémentaires sur le LOT 2 : MARKETPLACE et le LOT 3 : CONSEIL EN 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 consultation/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 exemple, consultation, services de migration, services gérés, opérations financières, etc.). Veuillez identifier les rôles pour lesquels vous formulez une offre :

LOT 1

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

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

____ – Fournisseur direct (CISP) de service 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/conseil fournissant des services pour l'utilisation ou l'exploitation sur un CISP

Indiquez le type d'offre :

- *Managed Services de charges de travail sur un CISP (O/N) : _____*
  - *Indiquez les spécialités le cas échéant : _____*
- *Services professionnels : (O/N) : _____*
- *Consultation – Formation (O/N) : _____*
- *Consultation – Stratégie (O/N) : _____*
- *Consultation – Migration (O/N) : _____*
- *Consultation – Gouvernance de cloud (O/N) : _____*
- *Consultation – Opérations financières (O/N) : _____*
- *Consultation – Autre (veuillez préciser) : _____*

Indiquez le ou les CISP pour lesquels 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 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 exemple, 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.*
Motifs d'exclusion, par exemple, 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 la commercialisation de nouveaux services et fonctions au cours des 5 dernières années, en particulier dans le domaine du PAAS, du machine learning et de l'analytique, du Big Data, des services gérés et des fonctions 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 à nos clients une infrastructure informatique de pointe sans avoir à effectuer de nouveaux investissements en capital.*

Relation entre le revendeur/partenaire et le CISP

*L'**<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 leur expertise. Ainsi, l'**<ORGANISATION>** n'a pas besoin d'examiner les Conditions et Services associés à une strate supplémentaire de sous-traitance entre le fournisseur principal de l'**accord-cadre** et le CISP. Cette exigence réduit également la complexité que génèrent les strates de revendeurs supplémentaires lorsque (1) l'**<ORGANISATION>** fait preuve de diligence raisonnable afin d'assurer une attribution claire des responsabilités concernant les services à fournir, et (2) l'**<ORGANISATION>** exerce les activités quotidiennes impliquant la consommation des services cloud.*

2.2 Technique

Un AO de services 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 cloud. Les CISP proposent des services standardisés à des millions de clients. Les personnalisations dans un AO de

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

services 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 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 séances d'exigences décrivent le processus commercial historique qui peut être vieillissant et inefficace. Si ces exigences sont ensuite intégrées à l'AO pour être 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 performances, mais ne doivent pas être prescriptives dans un appel d'offres en ce sens qu'elles dictent 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 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 dans un modèle de cloud, les actifs physiques ne sont pas achetés, il s'ensuit que de nombreuses exigences traditionnelles en matière d'approvisionnement des centres de données ne sont pas applicables. ***La réutilisation des questions du centre de données 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 cloud se concentre sur les exigences clés requises de la part d'un CISP et de services 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 : fonctionnalités 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 centres de données. Chaque cluster doit comprendre au moins 2 centres de données connectés par une liaison à faible	*Le CISP doit pouvoir offrir une infrastructure capable de créer des applications hautement disponibles, où des points de défaillance uniques peuvent être évités.*

temps de latence, afin de permettre des déploiements actif-actif hautement disponibles et des implémentations de scénarios de reprise après sinistre/continuité des opérations. Les centres de données comprenant chaque cluster doivent être physiquement isolés et indépendants les uns des autres en termes de pannes.	
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 imposent que le client contrôle entièrement l'emplacement de ses données.*
Le CISP doit pouvoir fournir une connectivité directe, dédiée et privée entre ses centres de données.	*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 être conforme au code de conduite sur la protection des données du CISPE, afin de fournir des fonctions et des services pouvant être utilisés en conformité avec le GDPR, qui permettent aux clients de créer des applications conformes au GDPR.	*Le client doit être en mesure de créer ou d'exécuter des applications en conformité avec le GDPR.*
Le CISP doit mettre à disposition des rapports audités par des tiers, tels que les rapports SOC 1 et 2 (couvrant les emplacements 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.*
Le CISP doit adhérer au Pacte pour un centre de données climatiquement neutre.	*Le Pacte pour la neutralité climatique des centres de données engage le CISP à atteindre la neutralité climatique d'ici 2030, et donc à permettre à l'utilisateur de soutenir ses propres objectifs de durabilité. Les auditeurs tiers sont obligatoires pour les fournisseurs >250 FTE (non PME).*
Le CISP doit adhérer au Code de conduite de portabilité IaaS SWIPO.	*Ce code garantit que les services répondent aux règles de l'Art. 6 « Portage de données » du règlement sur la libre circulation des données non personnelles.*
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'objets, une base de données relationnelle	*La simple offre de machines virtuelles ne suffit pas à qualifier un fournisseur de fournisseur de cloud.*

gérée, une base de données non relationnelle gérée, des équilibreurs de charge gérés, la surveillance et l'Auto Scaling intégré.	*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.	*Le paiement en fonction de l'utilisation permet au client d'optimiser ses charges de travail en termes de coût, de réduire 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 effectue lui-même l'opération.	*Le client doit contrôler l'emplacement 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 charges de travail. 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 la charge de travail, 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 charge de travail, environnement et compte.	

Le CISP doit également fournir des réponses aux questions d'exigence technique ci-dessous.

SOLUTIONS

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

- *Stockage*
- *DevOps*
- *Sécurité et conformité*
- *Big Data/Analytique*
- *Applications métier*
- *Télécommunications et réseaux*
- *Géospatial*
- *IoT*
- *[Autre]*

Présentez la façon dont le CISP a été utilisé pour les charges de travail 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 des fournisseurs

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

Les AO de services 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 pré-configurées via le CISP, ou des fonctions 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 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 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., calcul 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 des fournisseurs

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

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

1) ***Libre-service à la demande :** le soumissionnaire doit offrir la possibilité de fournir de manière unilatérale les compétences de calcul, 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 d'approvisionnement 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 :** le soumissionnaire doit fournir plusieurs options de connectivité réseau, dont une qui 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 soumissionnaire doit fournir des ressources de calcul regroupées qui servent plusieurs consommateurs à l'aide d'un modèle de multi-locataires avec différentes ressources virtuelles attribuées de manière dynamique et réattribuées en fonction de la demande des consommateurs. L'utilisateur est en mesure d'indiquer l'emplacement à un niveau d'abstraction supérieur (par ex., pays, région ou emplacement du centre de données). Le soumissionnaire doit prendre en charge la mise à l'échelle 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) ***Élasticité rapide :** le CISP du soumissionnaire doit prendre en charge les fonctionnalités d'approvisionnement et de désapprovisionnement du service (montée en charge et baisse en charge), pour rendre le service disponible dans les délais prescrits minimaux (maximum « x » heures) à compter de la demande d'approvisionnement. Le soumissionnaire doit prendre en charge les ajustements de facturation résultant de ces demandes d'approvisionnement quotidiennes, par heure ou par jour.*

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 cloud, comme le démontre le rapport Gartner Magic Quadrant pour IaaS[5].*
- *Indiquez des rapports d'analyste tiers reconnus du 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.

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

2.2.2.1 Contrats de niveau de service (SLA)

Les CISP proposent des SLA commerciaux standardisés à des millions de clients. À la différence des modèles de centre de données 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 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 : contrats de niveau de service (SLA)

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

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

*L'**<ORGANISATION>** sera responsable du maintien du SLA approprié associé 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 doivent refléter le fonctionnement d'un modèle de services 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 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 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 fonctions améliorées avant la publication de la prochaine version d'un accord-cadre. C'est pourquoi nous vous recommandons fortement d'étendre la fourniture 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'un codebase commun 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 cloud. Si de tels ajout, modification ou suppression sont effectués, les spécifications du service cloud doivent être modifiées en conséquence.*

*La portée de cet ordre de livraison comprend tous les services CISP existants, nouveaux ou améliorés **INCLUS DANS LE CHAMP D'APPLICATION DU CADRE.** Les services cloud fournis par le CISP et disponibles pour les clients commerciaux doivent être mis à la disposition de l'**<ORGANISATION>**.*

2.2.3.2 *Dépendance vis à vis du fournisseur/Réversibilité*

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

Cependant, un certain degré de dépendance vis à vis du fournisseur est inévitable lors de l'achat de services 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 fonctions 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.

Voir la section 2.3.1.2 pour des informations sur les Codes de conduite du secteur concernant le « portage des données » et le « changement de fournisseur de services cloud », afin de satisfaire aux exigences de l'article 6 du « Règlement sur la libre circulation des données à caractère non personnel » de l'UE.

Exemple de texte d'AO : intégration et départ

*L'**<ORGANISATION>** cherche à recevoir des propositions fournissant une stratégie de sortie raisonnable, afin d'éviter la dépendance vis à vis du fournisseur. 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 à partir de la plateforme du CISP, réduisant ainsi la dépendance. 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 fonctions de sécurité supplémentaires. Le niveau de 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 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 consultation/ISV et leurs solutions pour apporter leur aide.

2.3.1 Exigences minimales

En termes de sécurité dans le cloud, le mot-clé est **Fonctionnalités**. Les organisations du secteur public doivent être exigeantes vis à vis des CISP et exiger qu'ils fournissent les fonctionnalités de sécurité nécessaires pour que les clients puissent endosser leurs responsabilités dans le modèle de responsabilité partagée. Comme indiqué 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 de cloud unique.

- ***Fournir** des pares-feu de réseau et des **fonctionnalités** 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** d'implémenter une stratégie de défense approfondie et de contrer des attaques DDoS.*
- ***Fonctionnalités** de chiffrement des données disponibles dans les services de stockage et de base de données.*
- ***Fournir** des **options** de gestion des 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 au fil du temps.*
- ***Fournir des outils et fonctions** 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 quel emplacement émanent ces appels.*
- ***Fournir** des **options** d'agrégation de journaux, des enquêtes de rationalisation et des rapports de conformité.*

- *Donner la possibilité de configurer des notifications d'alerte lorsqu'un événement spécifique se produit ou que des seuils sont dépassés.*
- ***Fournir des fonctionnalités** pour définir, renforcer et gérer les stratégies d'accès utilisateur sur tous les services CISP.*
- ***Donner** la **possibilité** de définir des comptes utilisateur individuels avec des autorisations pour les ressources CISP.*
- ***Donner** la **possibilité** d'intégrer et d'associer des répertoires d'entreprise pour réduire le coût 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 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 porte sur les contrôles spécifiques auxquels un CISP adhère selon les exigences ISO relatives à l'acquisition, au développement et à 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 cloud.

Cette approche d'exploitation des rapports de conformité tiers peut être appliquée à la plupart des contrôles de conformité et de sécurité, par exemple, Code de conduite RGPD CISPE, 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>** dans le domaine de la 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 de cloud.*
- *Fournir des réponses aux spécifications techniques dans l'**ANNEXE A** des exigences de sécurité de l'**<ORGANISATION>**.*

PROPRIÉTÉ ET CONTRÔLE DU CONTENU DE L'<ORGANISATION>

*Décrire comment les fonctionnalités 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 solide, 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 fonctions d'accès, de chiffrement et de journalisation, 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 régions dans 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 régions choisies, sauf en cas d'obligation juridique 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 au repos, 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 l'environnement de contrôle de la sécurité du CISP. Les éléments de protection de la sécurité et processus de contrôle doivent être validés par plusieurs évaluations indépendantes de tiers.*

Les évaluations et les certifications d'accréditation de 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 de 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 centres de données 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 normes reconnues, dérivées des bonnes pratiques dans les opérations de service de cloud (y compris la gestion des données, leur sécurité, la confidentialité, la disponibilité, etc.), qu'elles soient opérationnelles, de sécurité ou de conformité, simplifient l'approvisionnement de la technologie de cloud.

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

Exiger que le CISP assure de façon continue le respect de la conformité selon la norme minimale 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)		
☐ CNDCP (Pacte sur la neutralité climatique des centres de données)		
☐ 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, Soins de 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*
☐ *Code IaaS SWIPO*		
	☐ *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 normes pouvant s'appliquer aux services cloud.

2.3.1.1 Protection des données

Une considération essentielle lors de l'utilisation de services cloud est que le traitement des données à caractère personnel est effectué conformément à la législation européenne applicable en matière de protection des données, y compris le Règlement général sur la protection des données (RGPD). Le RGPD est un règlement fondé sur des principes et ne fournit donc pas d'orientations sectorielles pour aider à assurer la conformité. Toutefois, le RGPD encourage l'adoption d'outils de conformité tels que des codes de conduite pour fournir de telles orientations. Le CISPE, en collaboration avec la Commission nationale de l'informatique et des libertés (CNIL), a élaboré un Code de conduite en matière de protection des données (code CISPE[6]), approuvé par le Comité européen de protection des données, qui s'applique de manière générale en Europe. L'objectif du Code est d'aider les CISP à se conformer au RGPD et de guider les clients dans l'évaluation de l'adéquation des CISP au traitement des données à caractère personnel que le client souhaite effectuer.

- Le Code se concentre exclusivement sur le secteur IaaS et aborde les rôles et responsabilités spécifiques des fournisseurs IaaS.
- Il contribue à clarifier les aspects du traitement équitable et transparent et des mesures de sécurité appropriées dans le contexte des services d'infrastructure de cloud (RGPD, article 40 [2]).
- Il aide les clients à comprendre comment ils peuvent conserver la souveraineté sur leurs données en s'assurant qu'elles restent dans l'UE.
- Il encourage les bonnes pratiques de protection des données qui soutiennent l'initiative GAIA-X de l'UE visant à développer des services européens de données en cloud.

Le respect par le CISP des codes de conduite en matière de protection des données, tels que le code CISPE, donne l'assurance que les à caractère personnel seront traitées dans le strict respect du RGPD.

[6] https://cispe.cloud/code-of-conduct/

Exemple de texte d'AO : protection des données

Le CISP faisant l'offre (directement ou par l'intermédiaire d'un revendeur) doit être en mesure de démontrer sa capacité à se conformer à un Code de conduite en matière de protection des données tel que le code CISPE. Le Code de protection des données doit s'aligner sur les exigences énoncées dans le cadre du RGPD. Le code doit contenir au minimum : (1) une définition claire des rôles et des responsabilités du CISP, (2) l'obligation pour le CISP de ne pas utiliser les données des clients à des fins de marketing ou de publicité, et (3) la possibilité pour les clients de sélectionner des services CISP permettant le traitement des données entièrement au sein de l'Espace économique européen. Le respect du code doit être vérifié par des auditeurs externes indépendants (organismes de contrôle) accrédités par des auditeurs externes indépendants accrédités par l'Autorité européenne de protection des données.

2.3.1.2 Changement de fournisseurs de cloud et portage des données

Les clients doivent avoir la liberté de choisir les services cloud qu'ils souhaitent utiliser, et ne pas être dépendants d'un CISP ou un fournisseur de PaaS/SaaS.

Les services cloud fournis par le CISP sont normalisés et offerts sur une base « un à plusieurs », les services étant configurés, fournis et contrôlés par le client. L'un des avantages du cloud computing réside dans le fait que les clients ont la possibilité de choisir les services standardisés dont ils ont besoin pour développer leurs applications et solutions uniques. Cet avantage s'étend à la possibilité de passer à des services nouveaux ou différents qui répondent mieux aux besoins du client à tout moment.

Comme pour la protection des données, les codes de conduite peuvent contribuer à rassurer les clients lorsqu'ils passent d'une infrastructure sur site à une infrastructure de cloud, ou lorsqu'ils changent de CISP. En collaboration avec EuroCIO (l'association européenne des CIO), le CISPE a co-présidé l'élaboration du Code de conduite pour la portabilité des données et le changement de service cloud pour les services cloud IaaS (Code IaaS SWIPO[7,8]). La première version du code a été élaborée conformément au règlement européen sur la libre circulation des données, remise à la Commission européenne en novembre 2019 sous la présidence finlandaise de l'UE et publiée par l'association SWIPO AISBL en mai 2020. En avril 2021, les premiers services ont été déclarés conformes au code par SWIPO AISBL, et en mai 2021, les premiers services membres de la CISPE ont été déclarés conformes au code.

Exemple de texte d'AO : changement de fournisseurs de cloud et portage des données

Le CISP faisant l'offre (directement ou par l'intermédiaire d'un revendeur) doit être en mesure de démontrer sa capacité à se conformer à un Code de conduite en matière de « commutation et de portage de données » tel que le Code IaaS SWIPO. Le code doit détailler la manière dont un CISP offre aux clients un transfert sûr de leurs données métier, s'ils décident de changer de CISP.

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security
[8] https://swipo.eu/

2.3.2 Comparaison des fournisseurs

Comme pour les critères techniques dans les sections ci-dessus, en plus des exigences de sécurité minimales dans un AO de services 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 posture de 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, allouer 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*
- *Fonctions pour des audits continus et en temps réel*
- *Capacité à créer un scripting technique des politiques de gouvernance du cloud*
- *La possibilité de créer des fonctions de contraintes qui ne peuvent pas être remplacées par des utilisateurs qui ne sont pas autorisés à modifier ces fonctions*
- *Capacité à mettre en œuvre de façon fiable les éléments contenus auparavant dans les politiques, les normes et les réglementations. Ils peuvent créer parallèlement une sécurité et une conformité applicables, ce qui génère en retour un modèle de gouvernance de 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 réduire les attaques sophistiquées de la couche application*
- *Service géré 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 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 fonctions 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 de disposer d'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 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 de 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 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.

Surtout, les AO de services cloud doivent étudier la valeur et le coût total de possession, 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 préqualification ou une liste de sélection de CISP, ceci accompagné des ***exigences minimales liées à la tarification****. Les CISP possédant des fonctionnalités similaires peuvent ainsi répondre aux critères de l'accord-cadre. Le processus d'évaluation pour les contrats exécutoires et les mini concours peut ensuite se porter 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. Des démonstrations de tests en direct sont également recommandées pour permettre de comparer les performances et l'élasticité des services de technologies de cloud fournis par les CISP. Consultez l'Annexe B pour accéder à un exemple de script de démonstration pour les technologies de cloud.*

2.4.1 Exigences minimales

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

1. **Tarification des services :** les clients du cloud intègrent un modèle d'utilisation avec paiement à 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 surveillance et de prédiction qui permettent aux clients de (1) contrôler 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 et (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 fonctionnalité de cloud commercial.

Le CISP doit fournir :

- *Un document contenant les définitions de service ou des liens vers les définitions de service*
- *Un document contenant les conditions générales*
- *Un document de tarification (les liens vers la tarification publique 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. 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 la capacité de mise à l'échelle 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 du CISP mesuré 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 de facturation/rapports de facturation
Pour démontrer la fourniture 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 fonctions et outils de budgétisation et de facturation fournies par le CISP, afin de respecter les exigences uniques de prédiction et de génération de rapports.

- *Fournir des informations sur la manière dont l'<ORGANISATION> peut consulter les informations de facturation aux niveaux complet et récapitulatif, en visualisant les schémas de dépenses des ressources CISP au fil du temps, en plus de prédire 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 sur 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 des 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 de la tarification des contrats exécutoires ou mini concours d'accord-cadre, il est important de créer une approche prenant en compte les fonctions uniques du cloud. Par exemple, il faut comprendre que la simple comparaison des postes entre les offres des fournisseurs de cloud (par ex. calcul ou stockage) n'est pas un moyen de comparaison efficace, car il ne prend pas en compte les fonctions telles que la performance, l'optimisation des coûts grâce aux services natifs cloud et outils de surveillance 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 cloud (y compris les services de partenaires, les remises CISP standardisées, les fonctions 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 centres de données dans des clusters au sein d'une région géographique. Un CISP qui ne possède pas ce type de redondance et de configuration de centre de données 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 globale de la tarification, tenant compte des fonctions techniques supplémentaires, est essentielle pour évaluer les CISP.

Exemple : un client veut comparer le prix du stockage d'objets 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 de deux unités, 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 peut 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 sur la durée de propriété du projet ou de la charge de travail global, et de la manière dont les fonctions 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 prix 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 doivent 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 fonctionnalités fondamentales d'un CISP est essentielle pour les clients du 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 fonctions « 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/différenciée et les remises disponibles commercialement, comme les instances réservées/instances Spot. Par exemple :

- x % d'économies si les clients achètent une capacité de calcul réservée (1 an, 3 ans, etc.)
- x % de remise sur la tarification différenciée/au volume
- x % d'économies d'après les révisions de l'architecture et l'optimisation de l'infrastructure, comme le basculement vers une option de calcul 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 charges de travail similaires, qui ont optimisé leurs dépenses sur 1/2/3 ans, grâce à l'utilisation des outils de surveillance et d'optimisation du CISP, en adoptant des solutions cloud natives 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 par leur conception. Les conditions contractuelles le sont donc également. Cependant, il est possible d'adapter légèrement ces contrats en fonction des contextes législatifs et réglementaires locaux.

Généralement, 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 de 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 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 de 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 portant sur 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 d'origine via l'AO de services cloud. Les CISP ajoutent constamment de nouveaux services et de nouvelles fonctions. 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 pré-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 informer 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 centre de données, des services gérés, du matériel, des logiciels prêts à l'emploi et de l'intégration système traditionnels. Leurs modèles économiques, uniques et impliquant une innovation constante, requièrent que le processus d'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 un problème, les deux équipes 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 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 emplacement et fournit des outils pour veiller à ce que le choix des emplacements 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 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 les meilleures technologies et solution.

Notez que les technologies cloud des CISP sont entièrement standardisées et fournies 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 fournisseurs représentants 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 comporteront 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 cloud est telle que les améliorations de service deviendront disponibles de manière permanente, ce qui peut permettre d'apporter plus d'efficacité aux clients.*
- *Les contrats 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 fourniture 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 le 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 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 l'emplacement géographique où elles sont conservées. Cela permettra aux clients d'éviter de dépendre d'un fournisseur et de déplacer librement les données vers de nouveaux fournisseurs.*

2.5.2 Conditions générales relatives aux logiciels

Bien que ce manuel porte sur l'achat de technologies de cloud IaaS et PaaS telles que fournies par un CISP, il est important de souligner les conditions des logiciels que les organisations du secteur public peuvent prendre en compte lors de l'achat de logiciels auprès de fournisseurs. Veuillez vous référer à la figure 1 (page 6) pour savoir comment les logiciels sont achetés dans le cadre d'une demande de propositions de services cloud bien structurée.

Les logiciels jouent un rôle essentiel dans presque toutes les entreprises, y compris dans le secteur public. L'inclusion d'obligations telles que les conditions d'octroi de licences de logiciels dans un appel d'offres de services cloud contribue à garantir que les entités du secteur public bénéficient de la meilleure valeur et ont la liberté de choisir leurs fournisseurs lors de l'achat de logiciels.

Consultez les dix principes pour l'octroi de licences logicielles équitables pour les clients utilisant le cloud[9] pour plus d'informations. Les principes ont été établis par Cigref[10], une association de grandes entreprises et d'administrations publiques françaises représentant les utilisateurs des technologies numériques, en collaboration avec CISPE, et avec le soutien d'autres associations professionnelles européennes de CIO et de fournisseurs, pour s'attaquer aux pratiques que les deux associations considèrent comme nuisant à la transformation numérique des organisations de toutes tailles lorsqu'elles passent au cloud.

Exemple de texte d'AO : logiciels

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>.*

Exigence 1.0. *Les fournisseurs de logiciels doivent fournir des conditions de licence claires, y compris une ventilation des coûts aux niveaux récapitulatif et granulaire.* ***Exigence 1.1.*** *Tous les frais relatifs au non-respect des conditions de la licence doivent être fournis aux niveaux récapitulatif et granulaire.*
Exigence 2.0. *Les licences logicielles doivent fournir à l'<Organisation> la possibilité de migrer le logiciel sous licence à partir du site vers le cloud de son choix, sans nécessiter l'achat de licences distinctes et dupliquées pour le même logiciel.* ***Exigence 2.1.*** *Les licences de logiciels doivent être exemptes de restrictions de licence et de coûts accrus qui limitent la capacité de l'<Organisation> à exécuter le logiciel sous licence dans le cloud de leur choix.*
Exigence 3.0. *Les licences de logiciel doivent permettre à l'<Organisation> d'exécuter le logiciel sous licence sur son propre matériel (généralement appelé logiciel « sur site »), ainsi que dans le cloud de son choix.*
Exigence 4.0. *Les licences de logiciel ne doivent pas exiger que le logiciel sous licence ne fonctionne que sur du matériel dédié uniquement à l'<Organisation>.*

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

Exigence 5.0. *Les éditeurs de logiciels ne doivent pas pénaliser l'<Organisation> si le logiciel sous licence de l'éditeur est utilisé sur l'offre de cloud d'un autre fournisseur, par exemple, en incluant des droits pour entreprendre des audits logiciels accrus ou intrusifs, ou imposer des frais de licence de logiciel plus élevés.*
Exigence 6.0. *Les logiciels d'annuaire doivent prendre en charge des normes ouvertes pour la synchronisation et l'authentification des identités des utilisateurs de manière non discriminatoire avec d'autres services d'identité.*
Exigence 7.0. *Les fournisseurs de logiciels ne doivent pas facturer des prix différents pour le même logiciel en fonction uniquement du propriétaire du matériel sur lequel il est installé.* ***Exigence 7.1.*** *Les prix des logiciels ne doivent pas faire de discrimination entre les logiciels installés dans le propre centre de données de l'<Organisation>, dans un centre de données géré par un tiers, sur des ordinateurs loués à un tiers, ou chez le fournisseur de cloud choisi par l'<Organisation>.*
Exigence 8.0. *Pendant la durée du contrat, les fournisseurs de logiciels ne doivent pas apporter de modifications importantes aux conditions de la licence qui restreignent l'<Organisation> par rapport aux utilisations précédemment autorisées, sauf si la législation l'exige ou en raison de problèmes de sécurité.*
Exigence 9.0. *Les fournisseurs de logiciels ne doivent pas induire en erreur l'<Organisation> en garantissant que les licences de logiciels couvriront l'utilisation prévue du logiciel par l'<Organisation>, telle que décrite dans les <Exigences de l'organisation>, alors que la couverture d'une telle utilisation peut nécessiter l'achat de licences supplémentaires.*
Exigence 10.0 *Si l'<Organisation> a le droit de revendre et de transférer des licences de logiciels, les fournisseurs de logiciels doivent continuer à offrir un support et des correctifs à des conditions équitables à l'<Organisation> qui a légalement acquis une licence revendue.*

2.5.3 Comment choisir un soumissionnaire par projet

Les organismes du secteur public qui sont parties au cadre peuvent commander ou « appeler » les services dont ils ont besoin lorsque cela est nécessaire. 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 contrat exécutoire, tout en conservant les avantages de l'accord-cadre.

Si nécessaire, un mini concours peut être organisé, afin d'identifier le meilleur fournisseur pour une charge de travail ou un projet en particulier. Au cours d'un mini concours, 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 compétents du lot à soumissionner, d'où l'importance des exigences minimales pour les soumissionnaires d'un appel d'offres de services cloud, car elles garantissent un niveau élevé d'options dans 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 de faisabilité technique et de compatibilité.

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

2.5.4 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 Bonnes 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 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, de (2) centraliser la gestion de toutes ces ressources et de (3) créer des alertes concernant leur utilisation/facturation/sécurité/etc. Tous ces avantages essentiels du cloud permettent aux clients de disposer d'une architecture optimisée (et dans la mesure du possible, automatisée) sans avoir à continuellement acheter 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.

Une façon utile de considérer un cloud CISP est qu'il s'agit effectivement d'une très grande API. Pour lancer un nouveau serveur ou modifier un paramètre de sécurité, il suffit d'effectuer des appels d'API. Toute modification apportée à l'environnement est journalisée et enregistrée (auteur, objet, emplacement et 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, au vu 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 agilité d'adaptation sera un processus évolutif, programme par programme. Ces expériences doivent être partagés, 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 dans un seul poste (calcul, stockage, réseaux, base de données, IoT, etc.), appelé Technologies de 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 et optimise ainsi l'utilisation et les faibles coûts.

Les organisations du secteur public peuvent ajouter des postes pour les commandes d'autres lots dans un cadre de cloud, si elles ont besoin de services de consultation/professionnels ou gérés, 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 de cloud à des services de consultation/professionnels/gérés dans un seul poste, il est possible de créer un poste « Technologies de cloud et de tâches auxiliaires ».

Voici ci-dessous un exemple représentatif de cette approche. Dans l'exemple ci-dessous, chaque unité du poste « #1001 – Technologies cloud » est égal 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'ÉLÉMENT	RESSOURCES/SERVICES	QUANTITÉ	UNITÉ	PRIX UNITAIRE	MONTANT
1001	Technologies cloud	1 000	Chacun	1 €	1 000 €
1002	Services de conseil	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 technologie 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 contrôlés grâce aux outils de surveillance et de prédiction du CISP. S'il reste peu d'argent, l'organisation demande des fonds supplémentaires au directeur financier, qui pourront être dédiés au maintien des services.

Exemple de texte d'AO : tarification – 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 service 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 de cloud ».

Chaque unité du poste commandé sera équivalent à <1,00 €> de technologies cloud commandées. Des commandes progressives 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 de 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'élément	Description	Qté	Unité	Prix
01	Technologies de cloud CISP	1 000	Chacun	1 000 €

MINIMUM DE COMMANDE/COMMANDE PROGRESSIVE
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 de cloud par l'<ORGANISATION>. Ces dispositions offriront à l'<ORGANISATION> la flexibilité nécessaire pour précommander <10 000> unités de « technologies de 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 totales de poste qui peut être commandé dans une seule commande progressive 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 économique du partenaire

Les entités du secteur public doivent comprendre les modèles selon lesquels les CISP proposent leurs offres, et que les partenaires qui fournissent des services de consultation, des services gérés, des

services de revente et plus encore, sont essentiels au processus. De nombreux clients nécessitent un fournisseur de cloud pour leur infrastructure et sous-traitent les tâches de planification, de migration et de gestion à un intégrateur système ou à un fournisseur de services gérés. 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'approvisionnements, 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 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 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 de dépendance vis à vis 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 fonctionnalité (il n'existe pas pierre de Rosette pour le cloud). Enfin, cette approche peut augmenter inutilement la complexité entre les clients du secteur public et leurs services cloud, ce qui peut compromettre la rentabilité et les gains de sécurité qu'ils cherchent à obtenir, et limiter la capacité de mise à l'échelle 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 cloud, elle doit inclure les parties prenantes de tous les aspects de l'organisation : direction, parties prenantes commerciales, technologie, finance, 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 sur le 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 cloud finalisé.

3.6 Développement durable

La durabilité est inhérente au cloud computing, et le passage au cloud permet de gagner en efficacité énergétique, par rapport aux serveurs sur site ou aux centres de données d'entreprise. L'identification d'un CISP qui donne la priorité à la durabilité et qui s'est engagé publiquement à atteindre des objectifs de durabilité fournit une assurance supplémentaire que le cloud est durable. Les CISP et les opérateurs de centres de données européens (avec le soutien de la Commission européenne) ont créé le Pacte pour des centres de données climatiquement neutres[11], une initiative d'autorégulation visant à établir des critères de durabilité clairs, simples et de grande portée pour le secteur des centres de données et à garantir que les opérateurs de centres de données et les fournisseurs de service cloud soient climatiquement neutres d'ici 2030. L'initiative d'autorégulation comprend des objectifs clairs d'efficacité énergétique des centres de données, de conservation de l'eau, de réutilisation et de réparation des serveurs, et d'utilisation d'une énergie sans carbone pour alimenter les centres de données. Les CISP qui s'inscrivent à l'initiative d'autorégulation acceptent de respecter ces objectifs et de se conformer aux critères pour être considérés comme un opérateur climatiquement neutre.

Un appel d'offres pour des services cloud doit demander aux CISP s'ils se sont engagés à respecter ces critères, en leur demandant spécifiquement s'ils ont adhéré à l'autorégulation et quand ils ont pris un tel engagement.

Exemple de texte d'AO : durabilité

Vous êtes-vous engagé à exploiter des centres de données climatiquement neutres en signant l'initiative d'autorégulation des centres de données climatiquement neutres ? Si oui, quand êtes-vous devenu signataire ?

Pouvez-vous fournir la preuve que vous avez obtenu le sceau du Pacte pour un centre de données climatiquement neutre pour l'utiliser ?

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

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 concours dans un accord-cadre de cloud.

1. Profil de fournisseur de 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 centres de données 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 centres de données 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 centres de données 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 centres de données conçus de manière à rester isolés en cas de pannes subies dans d'autres centres de données, avec une alimentation, des réseaux et un refroidissement redondants ?*
6.	*RÉPLICATION DE CENTRE DE DONNÉES :* *Le fournisseur de cloud offre-t-il une réplication des données entre les centres de données 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 Calcul

	Exigence
1.	*CALCUL – INSTANCE STANDARD – POLYVALENTE :* *Le fournisseur de cloud offre-t-il les types d'instance suivants ?* • *Polyvalente : type d'instance optimisé pour les applications génériques et qui fournit un équilibre entre les ressources de calcul, de mémoire et de réseau.* o *Si oui, quelle est la plus grande instance ?*
2.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – 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 calcul.* o *Si oui, quelle est la plus grande instance ?*
6.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – PRISE EN CHARGE DE PLUSIEURS CARTES RÉSEAU :* *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.	*CALCUL – 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 centre de données ?*
13.	*CALCUL – 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 centres de données au sein d'une région ?*
14.	*CALCUL – ALLOCATION EN LIBRE-SERVICE :* *Le fournisseur de cloud fournit-il l'allocation 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.	*CALCUL – 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.	*CALCUL – 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 utilisateur unique disponible ?*
17.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – 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 puissance) ?*
20.	*CALCUL – 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.	*CALCUL – 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 un texte d'instance, et de l'exporter dans un format de machine virtuelle ?* • *Si oui, quels sont les formats pris en charge ?*
22.	*CALCUL – INTERRUPTION DE SERVICE :* *Le fournisseur de cloud offre-t-il des mécanismes pour éviter des interruptions d'instances ou temps d'arrêt lorsque le fournisseur effectue une opération de maintenance de matériel ou de service au niveau de l'hôte ?*
23.	*CALCUL – REDÉMARRAGE D'INSTANCE :* *Le fournisseur de cloud offre-il des mécanismes pour redémarrer automatiquement les instances sur un hôte à l'état en cas de défaillance de l'hôte physique d'origine ?*
24.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – MÉCANISME DE SAUVEGARDE ET DE RESTAURATION :* *Le fournisseur de cloud offre-il un mécanisme intégré de sauvegarde et de récupération ?*
27.	*CALCUL – MÉCANISME D'INSTANTANÉ :* *Le fournisseur de cloud offre-il un mécanisme d'instantané manuel ou à la demande ?*
28.	*CALCUL – MÉTADONNÉES :* *Le fournisseur de cloud offre-t-il un service de métadonnées d'instance qui autorise les utilisateurs à définir des paires clé-valeur arbitraires pour l'instance ?*
29.	*CALCUL – APPEL DE MÉTADONNÉES :* *Le fournisseur de cloud offre-t-il un service de métadonnées d'instance qui fournit une interface de programme d'application (API) que l'instance peut appeler pour trouver des informations la concernant ?*
30.	*CALCUL – 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 charges de travail non stratégiques ?*
31.	*CALCUL – MÉCANISME DE PLANIFICATION :* *Le fournisseur de cloud offre-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.	*CALCUL – MÉCANISME DE RÉSERVATION :* *Le fournisseur de cloud offre-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.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – 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.	*CALCUL – SERVICE LIMITS :* *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des Service Limits) 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 Réseaux

	Exigence
1.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – PLUSIEURS PROTOCOLES :* *Le fournisseur 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – PRISE EN CHARGE DES JOURNAUX DE FLUX :* *Le fournisseur de cloud offre-t-il la possibilité de capturer les journaux de flux réseau ?*
18.	*RÉSEAUX – NAT :* *Le fournisseur de cloud fournit-il un service géré 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 cloud, tout en empêchant Internet d'établir une connexion à ces instances ?*

19.	*RÉSEAUX – VÉRIFICATION ORIGINE/DESTINATION :* *Le fournisseur de cloud a-t-il la possibilité de désactiver les vérifications origine/destination sur les cartes d'interface réseau (cartes réseau) ?*
20.	*RÉSEAUX – PRISE EN CHARGE DES VPN :* *Le fournisseur de cloud prend-il en charge la connectivité de réseau VPN entre le centre de données de l'utilisateur et lui-même ?*
21.	*RÉSEAUX – TUNNELS VPN :* *Le fournisseur de cloud prend-il en charge plusieurs connexions de réseau VPN par réseau privé ?*
22.	*RÉSEAUX – PRISE EN CHARGE DES VPN IPSec :* *Le fournisseur de cloud permet-il aux utilisateurs d'accéder à des services 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.	*RÉSEAUX – PRISE EN CHARGE DU BGP :* *Le fournisseur de cloud utilise-t-il le protocole de passerelle frontière (BGP) pour améliorer le basculement entre tunnels virtual private network (réseau VPN) du protocole de sécurité Internet (IPsec) ?*
24.	*RÉSEAUX – CONNECTIVITÉ PRIVÉE DÉDIÉE :* *Le fournisseur de cloud offre-t-il un service de connectivité direct et privé entre les emplacements du fournisseur de cloud et le centre de données, le bureau ou l'environnement de colocation d'un utilisateur permettant ainsi des transferts de données volumineux et rapides ?*
25.	*RÉSEAUX – ÉQUILIBREUR DE CHARGE FRONTAL :* *Le fournisseur de cloud offre-il un service de répartition 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.	*RÉSEAUX – ÉQUILIBREUR DE CHARGE BACKEND :* *Le fournisseur de cloud offre-t-il un service de répartition de charge dorsal (privé) qui achemine le trafic vers des instances hébergées dans des sous-réseaux privés ?*
27.	*RÉSEAUX – ÉQUILIBREUR 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.	*RÉSEAUX – ÉQUILIBREUR 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.	*RÉSEAUX – AFFINITÉ DE SESSION POUR LES ÉQUILIBREURS DE CHARGE :* *Le fournisseur de cloud offre-t-il un service de répartition de charge qui prend en charge l'affinité de session ?*
30.	*RÉSEAUX – RÉPARTITION DE CHARGE BASÉ SUR LE DNS :* *Le fournisseur de cloud offre-t-il un service d'équilibrage de charge capable de répartition de charge du trafic vers des instances hébergées sur plusieurs hôtes qui appartiennent à un seul domaine ?*
31.	*RÉSEAUX – JOURNAUX D'ÉQUILIBREUR 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.	*RÉSEAUX – DNS :* *Le fournisseur de cloud offre-t-il un service de système de noms de domaine (DNS) hautement disponible et évolutif ?*
33.	*RÉSEAUX – 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.	*RÉSEAUX – ROUTAGE DNS BASÉ SUR L'EMPLACEMENT 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 l'emplacement géographique (c'est-à-dire que le service DNS répond aux requêtes DNS en fonction de l'emplacement géographique des utilisateurs) ?*
35.	*RÉSEAUX – 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 l'acheminement 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 d'échec de la ressource principale) ?*
36.	*RÉSEAUX – 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.	*RÉSEAUX – SURVEILLANCE DE L'ÉTAT DU DNS :* *Le fournisseur de cloud offre-t-il un service de système de noms de domaine (DNS) qui effectue des surveillances de l'état pour surveiller l'état et les performances des ressources ?*
38.	*RÉSEAUX – 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.	*RÉSEAUX – 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 distribuer du contenu avec une faible latence et des vitesses de transfert de données élevées ?*
41.	*RÉSEAUX – 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 périphéries avant son expiration, notamment des fonctions telles que l'invalidation d'objets et la gestion des versions d'objet ?*
42.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – CERTIFICATS CDN :* *Le fournisseur de cloud offre-t-il un service de réseau de diffusion de contenu (CDN) prenant en charge les certificats de protocole SSL (Secure Sockets Layer) personnalisés afin de diffuser du contenu en toute sécurité via le protocole HTTPS (Hypertext Transfer Protocol Secure) à partir d'emplacements périphériques ?*
47.	*RÉSEAUX – 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 périphéries régionaux dans le but de réduire la latence ?*
48.	*RÉSEAUX – 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.	*RÉSEAUX – 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.	*RÉSEAUX – POINTS DE TERMINAISON :* *Le service de réseaux 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.	*RÉSEAUX – SERVICE LIMITS :* *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des service limits) concernant la section réseaux 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 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 – MISE À L'ÉCHELLE :* *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'objets évolutif 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'objets 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 POLITIQUES :* *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 L'EMPLACEMENT 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 l'emplacement 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 multifacteur (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 – IDENTIFICATIONS :* *Le fournisseur de cloud offre-t-il la possibilité de créer et associer des Identifications 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 D'OBJETS – OPTIMISATION DES CHARGEMENTS :* *Le fournisseur de cloud a-t-il la possibilité d'acheminer des données à partir d'emplacements 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 de recherche structurée 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 de recherche structurée 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 centres de données 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 inaltérables ?*
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 de recherche structurée 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 – SERVICE LIMITS :* *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des service limits) 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 POLITIQUE :* *Le fournisseur de cloud offre-t-il un mécanisme pour tester les effets des politiques 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 multifacteur (MFA) comme couche supplémentaire de contrôle d'accès et d'authentification vers son infrastructure ?*

11.	***ADMINISTRATION – SERVICE LIMITS :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des service limits) 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 géré pour allouer, gérer et déployer des certificats Secure Sockets Layer (SSL) (protocole SSL)/Transport Layer Security (protocole 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 – LDAP :* *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 géré qui aide les utilisateurs à faire tourner, gérer et récupérer facilement des informations d'identification, comme de clés d'interface de programme d'application (API), 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 géré de détection des menaces ?*
25.	***SÉCURITÉ – SERVICE LIMITS :*** *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des service limits) 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*	
☐ CNDCP (Pacte sur la neutralité climatique des centres de données)		
☐ 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, Soins de 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*
☐ *Code IaaS SWIPO*		
		☐ *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 centre de données ci-dessous, requis auprès du fournisseur de service cloud publique. 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 centre de données 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 centre de données du CISP : les employés CISP qui accèdent régulièrement à un centre de données doivent recevoir des autorisations d'accès aux zones concernées du site selon leur fonction, 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 centre de données, 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 centre de données, 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 centres de données 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 centre de données 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 centre de données doivent faire partie des opérations régulières du centre de données du CISP.*

- *Équipement de sauvegarde 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 juridiques 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 multifacteur. 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 utilisation hors limites, 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 centres de données, en effectuant un contrôle approfondi pour confirmer 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 centre de données 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 centres de données 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 centres de données, être physiquement séparée des autres et avoir une alimentation et des réseaux redondants. Les zones de disponibilité doivent être reliées les unes aux autres avec un réseaux 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 entraînée 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 centre de données. Le CISP doit fournir des détails sur son engagement à utiliser une énergie renouvelable pour ses centres de données, et fournir des informations sur la manière dont ses clients peuvent réduire les émissions carbone par rapport à ses propres centres de données.*

- *Sélection de site : avant de choisir un emplacement, le CISP doit effectuer des évaluations initiales en matière d'environnement et de zone géographique. Les emplacements des centres de données 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 centres de données doivent être conçus pour anticiper et tolérer les échecs tout en maintenant les niveaux de service. En cas d'échecs, les processus automatisés doivent éloigner le trafic de la zone affectée. Les applications essentielles doivent être déployées selon le standard N+1 de manière à ce que, en cas d'échec d'un centre de données, 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 emplacement 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 centre de données en termes de zones de disponibilité et de réplication des données doit 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.*

SURVEILLANCE ET JOURNALISATION

- ***Vérification de l'accès au centre de données :*** *l'accès aux centres de données doit être régulièrement contrôlé. L'accès doit être automatiquement révoqué lorsque le dossier d'un employé est résilié 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 centre de données*** *: l'accès physique aux centres de données 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 centre de données :*** *le CISP doit surveiller les centres de données 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 centre de données, 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 centre de données :*** *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 centres de données. 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 des stocks qui stocke et suit le propriétaire, l'emplacement, l'état, la maintenance et les informations descriptives pour les ressources appartenant au CISP. Suite à l'approvisionnement, les ressources 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 Standards rigoureux 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 centres de données 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 centres de données soient équipés d'une alimentation de secours, afin de garantir qu'une alimentation soit disponible pour maintenir les opérations en cas d'échec électrique pour des charges critiques et essentielles dans les installations.

- ***Climat et température :*** *les centres de données 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 centres de données 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 réseaux, mécaniques et d'infrastructure. Ces zones doivent également être protégées par des systèmes de suppression.*

- ***Détection des fuites :*** *le CISP doit équiper les centres de données 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 centres de données 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 surveillance doit être effectuée grâce à des outils et informations d'audit continus, fournis via des systèmes de gestion des bâtiments et de surveillance 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 centre de données :*** *le centre des opérations de sécurité du CISP doit évaluer régulièrement les menaces et vulnérabilités des centres de données. L'évaluation et la limitation en cours des vulnérabilités potentielles doivent être effectuées grâce à des activités d'évaluation des risques du centre de données. 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 centres de données 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 centre de données, tester les appareils électroniques de contrôle de l'accès et examiner l'équipement du centre de données.*

7. Migrations

	Exigence
1.	*SERVICE DE MIGRATION :* *Combien de services de migration de données différents le fournisseur de cloud offre-t-il ?*
2.	*MIGRATIONS – SURVEILLANCE 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 surveillance 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 PROGRESSIVE DE SERVEUR :* *L'outil de migration du fournisseur de cloud offre-t-il une réplication progressive de serveur 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 sur 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 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 À L'ÉCHELLE DU PÉTAOCTET :* *Le fournisseur de cloud offre-t-il une solution de migration de données à l'échelle du pétaoctet qui utilise des composants sécurisés pour transférer des volumes importants de données depuis et vers le cloud ?*
22.	*MIGRATIONS – MIGRATION DE DONNÉES À L'ÉCHELLE DE L'EXAOCTET :* *Le fournisseur de cloud offre-t-il une solution de transport de données à l'échelle de l'exaoctet 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 centre de données 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'OBJETS :* *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 – SERVICE LIMITS :* *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des service limits) 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 créer 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 – SERVICE LIMITS :* *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des service limits) 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. Matériel

	Exigence
1.	***GESTION – SERVICE DE SURVEILLANCE :*** *Le fournisseur de cloud offre-t-il un service de surveillance 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 surveillance du fournisseur de cloud permet-il aux utilisateurs de configurer des alarmes ?*
3.	***GESTION – MÉTRIQUES PERSONNALISÉES :*** *Le service de surveillance du fournisseur de cloud permet-il aux utilisateurs de créer et surveiller des métriques personnalisées ?*
4.	***GESTION – GRANULARITÉ DE LA SURVEILLANCE :*** *Le service de surveillance du fournisseur de cloud offre-t-il différents niveaux de surveillance, 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'interface de programme d'application (API) 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 de l'interface de programme d'application (API) ?*
7.	***GESTION – COMPRESSION :*** *Le fournisseur de cloud offre-t-il un mécanisme permettant de compresser les journaux générés par le système de suivi d'une interface de programme d'application (API) 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'interface de programme d'application (API) 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 surveillance 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 surveillance des services cloud ?*
18.	*GESTION – ACCÈS À LA CLI :* *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 – SERVICE LIMITS :* *Le fournisseur de cloud est-il soumis à des restrictions (c.-à-d. des service limits) 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 – SERVICE HEALTH DASHBOARD :* *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 de compte technique (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 interface de programme d'application (API) 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 de l'utilisateur, des didacticiels, des questions fréquentes (FAQ) et des notes de mise à jour ?*
13.	*SUPPORT – DOCUMENTATION DE LA CLI :* *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 en ligne un ensemble gratuit de documents d'architecture de référence pour aider ses clients à créer des solutions spécifiques en combinant de nombreux services cloud qu'il propose ?*
15.	*SUPPORT – DÉPLOIEMENTS DE RÉFÉRENCE :* *Le fournisseur de services cloud offre-t-il en ligne 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 des données, charges de travail Microsoft, charges de travail SAP, etc.) dans ses offres cloud ?*

Annexe B – Évaluation technique en temps réel

Lors de la sélection d'un CISP (fournisseur de services d'infrastructure cloud), les capacités de la plateforme cloud doivent être évaluées « en temps réel » à l'aide des services et de l'infrastructure du CISP disponibles au public. Par CISP présélectionné, nous recommandons une évaluation technique couvrant au minimum une journée. Pendant l'évaluation, vous pouvez : 1) effectuer une évaluation approfondie pour déterminer si les capacités démontrées sont conformes aux exigences de votre demande de propositions et aux réponses écrites du CISP, 2) fournir une plateforme permettant à vos experts de sonder le CISP pour s'assurer de son adéquation et de son alignement avec vos besoins techniques et organisationnels spécifiques, et 3) avoir confiance dans les services du CISP et dans ses compétences en matière de mise à l'échelle, de sécurité et de résilience et continuer à innover pour répondre aux besoins futurs.

Lorsque les CISP répondent aux exigences d'une demande de services cloud, ils peuvent déclarer la conformité sur la base d'une interprétation de haut niveau des exigences, qui ne tient pas compte du contexte général de l'environnement opérationnel/des besoins d'application d'une organisation. Nous suggérons de constituer un panel d'évaluation technique en temps réel avec des experts éminents en matière de technique, d'exploitation, de sécurité et d'applications. Les évaluateurs doivent remettre en question le CISP tout au long de l'évaluation et, suivant la bonne pratique, ils doivent noter les CISP de manière indépendante, en notant les scénarios sur une échelle fixe, par exemple de 0 à 4 (0=Inacceptable, 1=Insuffisant, 2=Acceptable, 3=Bon, 4=Exceptionnel). Ensuite, les scores des démonstrations peuvent être consolidés. En effet, le score moyen de chaque scénario d'évaluation est repris dans l'évaluation globale du CISP. Les scénarios présentant un écart-type élevé doivent être examinés par l'équipe d'évaluation avant d'être validés. Une fois les scores consolidés, une pondération basée sur la nature de la critique des scénarios peut être appliquée.

Nous recommandons une approche globale de la plateforme du CISP, puis une évaluation plus approfondie des charges de travail spécifiques s'exécutant sur la plateforme, en fonction de la portée de la démonstration. Vous trouverez ci-dessous un exemple de plan d'évaluation de la plateforme et de la charge de travail. Les organisations peuvent s'appuyer sur cette base ou la personnaliser pour s'assurer que le CISP sélectionné répond à leurs exigences fonctionnelles et non fonctionnelles spécifiques. La bonne pratique consiste à autoriser les fournisseurs à qui l'on présente la liste des scénarios et des exigences à proposer un ordre du jour pour l'évaluation en temps réel qui maximise la couverture et prévoit 20 % de temps pour les questions et réponses.

Évaluation de la plateforme : plusieurs CISP ont adopté le concept « Well-Architected » pour désigner une approche du cloud qui offre une valeur optimale et minimise les risques. Les scénarios bien architecturés dans une démonstration technique en temps réel sont notamment les suivants :

1. Sécurité : identité, gouvernance centralisée, détection automatisée des menaces, protection des données, préparation aux événements.
2. Efficacité des performances : dimensionnement correct, capacité de mise à l'échelle/élasticité, sans serveur.
3. Fiabilité : haute disponibilité (résistance aux échecs), réduction des risques de changement, reprise après sinistre, sauvegarde.
4. Gestion des coûts : opérations financières, optimisation commerciale, budgets et allocation des coûts.
5. Excellence opérationnelle : automatisation, surveillance, assistance, gestion et capacités requises pour migrer vers le cloud et y fonctionner.

Évaluation de la charge de travail : parmi les types d'applications qui peuvent faire l'objet d'une démonstration, figurent les suivantes :

- Application web : hébergement public d'un site web dynamique, y compris la base de données backend et le stockage d'objets statiques.
- Analytique des données : une architecture Lake House ou de lac de données qui permet la consolidation des données provenant de fournisseurs de données disparates et la capacité de traiter un volume (To/Po de données), une variété (structuré, non structuré, différents formats, etc.) et une vélocité (taux de génération de données, changement et modèles de requête) élevés.
- Plateforme de science des données : une plateforme qui permet le développement, le déploiement et l'utilisation de capacités basées sur l'IA/ML à travers votre organisation.
- Application IoT : une plateforme/capacité IoT qui englobe le cloud, une capacité réseau et les appareils.

Pour chaque charge de travail représentative essentielle à votre organisation, vous pouvez définir les scénarios à démontrer par le CISP. Les scénarios doivent démontrer les capacités globales qui permettent le déploiement de la charge de travail d'une manière Well-Architected. Les pages suivantes comprennent des exemples de critères d'évaluation technique en temps réel pour : 1) la plateforme du CISP, et 2) un exemple de charge de travail d'application web.

Plateforme – Exemple d'évaluation technique en temps réel

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
Plateforme Sécurité 1	Fédération d'identités	4	Démonstration de la capacité de fédérer à partir d'une base d'identités existante vers le service cloud.	• Prise en charge de protocoles standard tels que SAML. • Prise en charge de la réplication d'identité basée sur SCIM. • Capacité de définir différents niveaux d'accès dans la base d'identités d'entreprise et de les faire appliquer par le fournisseur de services cloud. • Capacité de limiter des équipes/individus spécifiques à certains comptes/projets/charges de travail. • Capacité à prendre en charge le contrôle d'accès basé sur les attributs (ABAC) et à les utiliser dans le cadre du système Identity and Access Management (IAM) du fournisseur de services cloud pour contrôler l'accès aux ressources cloud.
Plateforme Sécurité 2	Gouvernance centralisée	4	Démonstration de la capacité à définir la politique et les exigences de manière centralisée, au niveau organisationnel (politiques globales) et des unités opérationnelles et des projets.	• Cette politique doit être conçue comme suit : activer/désactiver des services, appliquer des restrictions géographiques (limiter les régions). • Celles-ci doivent également empêcher les utilisateurs, y compris les administrateurs, de désactiver tout contrôle d'audit/de gouvernance.
Plateforme Sécurité 3	Limitation des autorisations des utilisateurs	3	Démonstration des recommandations automatiques pour le renforcement des autorisations des utilisateurs.	• Capacité de comparaison des autorisations actuelles par rapport à celles requises. • Génération automatique de politiques pour promouvoir le moindre privilège.
Plateforme Sécurité 4	Journalisation des audits	4	Démonstration de la journalisation d'audit de l'activité du cloud, incluant les actions autorisées et celles interdites.	• Journaux centralisés pour l'ensemble de l'organisation. • Journaux spécifiques au compte/projet pour assurer la traçabilité et la responsabilité au niveau inférieur. • Outils d'aide à la recherche des données dans les journaux.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
				• Outils d'aide au déclenchement des actions en fonction d'événements/entrées de journal spécifiques. • Capacité de consultation de l'activité du support fournisseur. • Capacité d'empêcher la suppression des journaux, même par les administrateurs.
Plateforme Sécurité 5	Isolement du réseau	4	Démonstration et preuve, au besoin, de l'isolation des différents locataires dans le cloud. Démonstration de la configuration de sous-réseaux isolés (sans connectivité), privés (sans Internet) et publics (avec accès à Internet).	• Séparation des locataires, y compris pour les services VPN et de connexion croisée. • Capacité à contrôler le flux de trafic depuis l'extérieur de l'infrastructure cloud (sur site), à l'intérieur de celle-ci et vers l'Internet. • Application de la séparation lors de l'utilisation de services partagés tels que l'hébergement de conteneurs ou la fonction en tant que service.
Plateforme Sécurité 6	Chiffrement au repos	4	Démonstration de la capacité de chiffrer les données au repos, y compris les options de chiffrement BYOK et côté client.	• Capacité d'exiger le chiffrement de données sensibles. • Capacité de gestion des clés gérées par le fournisseur ou par le client. • Adhésion à la norme FIPS 140-2. • Capacité d'alerte et de journalisation des cas de non-respect des exigences en matière de chiffrement. • Incidence sur les coûts supplémentaires. • Incidence sur les performances. • Prise en charge des algorithmes de preuve quantique et des valeurs de clés.
Plateforme Sécurité 7	Chiffrement en transit	4	Démonstration de la capacité de chiffrer les données en transit.	• Chiffrement par défaut pour les API de service. • Capacité d'activation du chiffrement en transit (TLS) sur les équilibreurs de charge et les API gérées. • Prise en charge de l'authentification mutuelle (client et serveur).
Plateforme Sécurité 8	Gestion des clés	4	Démonstration de votre capacité de gestion des clés. Inclure le cycle de vie	• Journalisation de la création, l'utilisation, la rotation et la destruction des clés.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
			complet de la clé. Inclure l'intégration avec les services cloud.	
Plateforme Sécurité 9	Gestion de la configuration	3	Démonstration de vos capacités de gestion de la configuration de la plateforme cloud.	• Tenir à jour le CMBD. • Contrôler la conformité. • Déclencher automatiquement des actions basées sur la non-conformité. • Capacité d'évaluation des changements de configuration par rapport aux bonnes pratiques ou aux règles personnalisées.
Plateforme Sécurité 10	Sécurité du réseau	3	Démonstration de la capacité du pare-feu d'application web et du pare-feu, y compris l'intégration avec des ensembles de règles/pare-feu tiers et la protection contre les attaques en volume.	• WAF (Pare-feu d'application web) : capacité de mise à l'échelle. • Prise en charge des réseaux privés et publics. • Capacité d'abonnement aux flux de l'industrie et des fournisseurs pour les ensembles de règles. • Déclenchement automatiquement des actions au sein de l'infrastructure en fonction des événements provenant du WAF. • Capacités de pare-feu, capacité de mise à l'échelle. • Pares-feu basés sur l'hôte et sur le réseau. • Capacité de référencement des groupes ou des objets logiques en plus de la possibilité de spécifier des blocs IP CIDR. • Nombre de règles prises en charge à chaque niveau/composant. • Capacité de prise en charge d'un modèle d'exploitation distribué (équipe réseau + équipe de développement) par le biais de la politique et de la configuration du réseau.
Plateforme Sécurité 11	Connectivité réseau	3	Démonstration de la capacité à se connecter à des réseaux sur site ainsi qu'à des points de terminaison/clients sur des réseaux privés dans le cloud.	• Connectivité privée (bande passante haut débit > 10Gb/s). • Capacité de contrôle des politiques de routage et de pare-feu dans l'ensemble de l'organisation.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
				• Connectivité VPN (de site à site et basée sur le client). • Support IPV6.
Plateforme Sécurité 12	Gestion des instances	3	Démonstration des capacités de gestion des instances.	• Capacité à surveiller et à gérer l'état des correctifs d'un gros volume d'instances. • Prise en charge de la gestion des correctifs pour les systèmes d'exploitation Linux et Windows. • Capacité d'exécution des commandes sur une flotte de serveurs sans avoir besoin de SSH. • Capacité de contrôle et d'audit de l'accès à distance aux machines virtuelles de manière centralisée. • Capacité de modifier la taille d'une instance, d'attacher des volumes supplémentaires, de modifier la configuration du réseau, etc. par le biais de la console, de la CLI et de l'API.
Plateforme Sécurité 13	Application de la politique	3	Démonstration de la capacité à configurer les services pour empêcher l'accès depuis l'Internet public.	• Capacité d'isoler le trafic vers un réseau privé pour les services susceptibles de contenir des données critiques/confidentielles. • Capacité de définir des politiques qui contrôlent l'accès aux données en fonction du réseau source. • Application de ces restrictions d'accès à tous les utilisateurs, y compris ceux disposant d'informations d'identification de niveau supérieur.
Plateforme Sécurité 14	Recherche de vulnérabilités	2	Démonstration de la capacité à analyser les images (conteneur et VM) à la recherche de vulnérabilités.	• Capacité à analyser automatiquement les conteneurs dans un registre. • Capacité à analyser les machines virtuelles à la recherche de vulnérabilités connues. • Capacité à effectuer un balayage du réseau.
Plateforme Sécurité 15	Inspection du réseau	2	Démonstration de la capacité de capturer/mettre en miroir le trafic réseau (NetFlow et le paquet complet) à partir d'un environnement client.	• Capacité à mettre en miroir une partie ou la totalité du trafic au sein de l'infrastructure du fournisseur de cloud (du point de vue du client locataire), avec capture complète des paquets.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
				• Capacité à sélectionner simplement le trafic que vous souhaitez capturer. • Capacité à mettre à l'échelle pour des volumes de trafic très importants (>50Gb/s).
Plateforme Sécurité 16	Détection des menaces	3	Démonstration de la capacité de détection d'intrusion de votre plateforme, notamment les menaces provenant d'un réseau, l'utilisation des informations d'identification et l'analyse des modèles d'utilisation, par exemple.	• Capacité à détecter les activités suspectes telle que le « data mining ». • Capacité à détecter les attaques d'authentification par forçage, comme les connexions SSH. • Capacité à détecter les fuites ou les abus relatifs aux informations d'identification. • Application du ML, permettant d'analyser un grand nombre d'événements et de faire apparaître les événements prioritaires. • Effort d'activation/configuration (il est préférable de faire simple). • Capacité d'intégrer des services externes et de déclencher des notifications. • Capacité de configurer l'IDS à un niveau global pour tous les projets/comptes.
Plateforme Performance 1	Optimisation des calculs	2	Démonstration des recommandations automatiques pour l'optimisation des coûts des machines virtuelles et des fonctions en tant que service.	• Recommandations fondées sur l'utilisation réelle et les modèles de charge de travail. • Les recommandations comprennent une estimation des économies et des informations sur le niveau de charge prévu et les implications techniques. • Les optimisations doivent inclure à la fois les économies et le « risque de performance » lorsque les machines virtuelles peuvent par exemple être sous-dimensionnées.
Plateforme Performance 2	Optimisation de l'environnement	2	Démonstration des recommandations automatiques pour d'autres composants du cloud tels que les	• Les recommandations identifient les économies et les possibilités d'amélioration des performances dans d'autres composants que le calcul central.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
			équilibreurs de charge, les réseaux, les bases de données, le stockage, etc.	
Plateforme Performance 3	Mise à l'échelle automatique des calculs	4	Démonstration des capacités de scalabilité automatique d'une application déployée derrière un équilibreur de charge dans un environnement de calcul virtuel. Démonstration des différentes options/approches disponibles et la possibilité de déclencher d'autres actions (facultatives) avant/après des événements de mise à l'échelle, comme une notification.	• Différentes options de mise à l'échelle, basées sur des déclencheurs, sur le temps, sur l'action manuelle ou sur des approches plus intelligentes qui appliquent le machine learning pour prédire la capacité requise. • Mise à l'échelle entièrement automatique, y compris l'enregistrement avec un équilibreur de charge et les surveillances de l'état. • La capacité d'exécuter un morceau de code arbitraire à des moments précis du cycle de vie de la mise à l'échelle.
Plateforme Performance 4	Mise à l'échelle en ligne pour le stockage	3	Démonstration de mise à l'échelle de la capacité et du débit de stockage en bloc sans interruption de la charge de travail.	• Capacité de faire passer le stockage en bloc d'un type de stockage à un autre sans avoir à recréer complètement les services. • Capacité à augmenter la taille des volumes présentés aux VMs.
Plateforme Performance 5	Mise à l'échelle automatique pour les Managed Services	3	Démonstration de la capacité du magasin d'objets, de l'API Gateway, de la plateforme FaaS et de la base de données NoSQL à changer d'échelle de quelques (10) à de nombreux (1 000) utilisateurs simultanés.	• Mise à l'échelle automatique transparente, idéalement sans intervention de l'administrateur. • Des performances constantes dans le cadre de l'augmentation d'échelle en phase avec les exigences de mise à l'échelle de la production. • Pour certains composants, comme FaaS, examinez les options de préchauffage et de gestion des limites d'exécution simultanée si besoin est.
Plateforme Performance 6	Charges de travail basées sur des conteneurs	3	Démonstration de la capacité à héberger des charges de travail basées sur des conteneurs.	• Options pour les plateformes d'hébergement de conteneurs. • Intégration avec d'autres composants IaaS tels que les équilibreurs de charge. • Disponibilité d'une solution de maillage de services.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
				• Options non propriétaires pour l'hébergement de conteneurs, telles que Kubernetes. • Prise en charge native de la haute disponibilité dans le plan de contrôle du conteneur. • Capacité de gérer les hôtes de conteneurs sur site.
Plateforme Fiabilité 1	Résilience des régions	4	Démonstration du basculement automatique d'une instance de base de données relationnelle dans une région lorsqu'un échec localisé géographiquement (telle qu'une panne de courant) est simulée.	• Basculement automatisé. • Zones de failles isolées dans une région cloud. • Démarcation précise et architecture simple pour la haute disponibilité.
Plateforme Fiabilité 2	Auto-récupération d'instance	2	Démonstration de la récupération automatique d'une instance / d'un ensemble d'instances après l'échec d'une surveillance de l'état.	• Surveillances de l'état configurables. • Récupération et réapprovisionnement des instances entièrement automatisés.
Plateforme Fiabilité 3	Surveillance de l' état de l' équilibreur de charge	3	Démonstration de la manière dont un équilibreur de charge détecte automatiquement une instance en panne et réachemine le trafic vers d'autres hôtes en état.	• Surveillances de l'état configurables. • Routage automatisé du trafic vers les hôtes en état.
Plateforme Fiabilité 4	Basculement de région	3	Démonstration d'une architecture multirégionale, incluant le basculement automatisé du trafic vers une région secondaire.	• Surveillances de l'état à l'échelle globale. • Options pour le routage automatisé : latence, pondération et basculement. • Prise en charge des charges de travail des machines virtuelles ainsi que des services gérés tels qu'un service de base de données de type Magasin d'objets/NoSQL.
Plateforme Fiabilité 5	Sauvegarde et restauration	4	Démonstration des options de sauvegarde et de restauration pour : les machines virtuelles, les bases de données, les services gérés.	• Niveau d'automatisation. • Capacité de restauration vers la même/une autre région du cloud. • Capacité de copie des sauvegardes vers une autre région du cloud.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
Plateforme Coût 1	Budgets	3	Démonstration d'une capacité de gestion budgétaire, notamment à travers le mode de structuration pour les sous-comptes et les projets.	• Étudier la possibilité d'appliquer des contrôles et une surveillance budgétaires aux différents niveaux de votre organisation. • Contrôler la flexibilité, par exemple la capacité de regroupement des composants (par étiquetage), de fixation des budgets pour des services cloud spécifiques et de configuration des seuils d'alerte/de surveillance.
Plateforme Coût 2	Allocation du budget	1	Démonstration de la mise à disposition d'un nouvel environnement de projet (compte), y compris le processus d'allocation budgétaire pour le projet. L'approvisionnement doit inclure des étapes d'approbation manuelle pour 1) la révision technique/IT, 2) la révision commerciale/Finance.	• Capacité d'auto-allocation moyennant les approbations appropriées. • Automatisation de la configuration de l'établissement du budget, des notifications ou des politiques budgétaires appropriées, en fonction de votre organisation.
Plateforme Coût 3	Rapports budgétaires	2	Démonstration de la capacité à établir des rapports sur les budgets dans l'ensemble de l'organisation. Rapports destinés à un service spécifique ou à l'ensemble de l'organisation (information nécessaire). Les rapports doivent inclure les valeurs de dépenses « réelles » ainsi que les valeurs de dépenses prévues/estimées.	• La capacité de fournir une visibilité à différents niveaux de l'organisation, en créant une prise de conscience et une transparence à condition essentielle d'un besoin d'information. • Les prédictions doivent être basées sur les tendances de consommation actuelles et passées et, fournir un avertissement précoce des dépassements de budget potentiels.
Plateforme Coût 4	Contrôles budgétaires	1	Démonstration de la capacité à prendre des actions lorsqu'un seuil budgétaire est atteint. Les actions peuvent inclure des notifications, l'application de contraintes ou une	• La capacité à définir des actions simplement pour différents projets. • La capacité de variation des actions d'un projet à l'autre, par exemple – en tenant compte des implications Dev vs. Prod.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
			intervention active pour prévenir les dépassements de budget.	• La capacité à définir plusieurs actions et seuils pour le même budget/projet. • La capacité à définir des actions personnalisées en plus des capacités standard.
Plateforme Coût 5	Périodicité du budget	1	Démonstration de la capacité à définir des budgets pour différentes périodes : quotidienne, mensuelle, annuelle, etc. Pour les budgets annuels, démontrer la capacité à définir une distribution variable des dépenses prévues tout au long de l'année.	• Capacité à définir des budgets pour différentes périodes. • Capacité à configurer une distribution des dépenses sur l'année pour les budgets annuels. Cette approche est particulièrement importante pour les charges de travail saisonnières/très élastiques, comme la déclaration fiscale annuelle par exemple.
Plateforme Coût 6	Marketplace tierce	3	Démonstration de la capacité d'acheter et de déployer des produits tiers. Démonstration de la procédure de fixation d'un budget pour un ensemble de produits tiers disponibles sur une plateforme de marché et de la possibilité de restreindre les produits disponibles.	• Capacité à définir un budget pour un produit spécifique, un budget global, un budget pour un ensemble de projets/comptes. • Capacité à ne présenter qu'un sous-ensemble du marché plus large aux utilisateurs du cloud.
Plateforme Coût 7	Modèles de tarification des calculs	3	Démonstration des différents modèles de tarification/commercialisation utilisables pour les machines virtuelles.	• Les capacités doivent inclure une tarification à la demande, sans engagement à long terme et granulaire (par minute/heure). • Engagements à long terme facultatifs en échange d'une remise. • Capacité à acheter des instances en consentant à être interrompu en échange d'une remise. • Autre point important, il devrait être possible de combiner ces modèles au sein d'un même projet/compte, et de partager les bénéfices entre différents comptes.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
Plateforme Coût 8	Recommandations pour l'optimisation commerciale	3	Démonstration de la capacité à recevoir des recommandations d'optimisation commerciale pour optimiser les dépenses (sans avoir à effectuer de changements techniques).	• Recommandations holistiques pour de multiples services, y compris pour les machines virtuelles et les bases de données gérées. • Capacité de mise en œuvre des recommandations de manière simple et à comprendre les économies/bénéfices escomptés.
Plateforme Coût 9	Hôtes dédiés	4	Démonstration de la capacité à allouer un hôte dédié pour permettre l'utilisation de licences sur site liées à un hôte spécifique.	• Facilité d'approvisionnement. • Capacité à gérer l'utilisation de l'hôte. • Capacité à partager l'hôte entre différents projets/locations.
Plateforme Opérations 1	Migration des machines virtuelles	3	Démonstration de l'importation d'une machine virtuelle depuis un site sur site vers un service de VM basé sur le cloud.	• Capacité à importer des systèmes d'exploitation basés sur Windows et Linux. • Capacité à importer plusieurs machines à la fois. • Capacité à maintenir une session de réplication pour permettre un « basculement » rapide vers le cloud.
Plateforme Opérations 2	Capacités DevOps et d'automatisation	4	Démonstration de vos capacités DevOps/automatisation, incluant le mode de configuration des environnements en tant que code, la prise en charge des déploiements entièrement automatisés, les tests automatisés et les restaurations.	• Capacité à définir tous les composants des systèmes en tant que code, y compris le réseau, les machines virtuelles, le stockage, les bases de données. • Capacité à créer un pipeline. • Capacité à créer un dépôt de code. • Capacité à automatiser les créations. • Capacité à effectuer des déploiements bleus/verts. • Capacité de créer des environnements multiples et d'avoir plusieurs étapes pour les déploiements. • Restauration automatique en cas d'échec des déploiements
Plateforme Opérations 3	Hébergement d'applications	2	Démonstration de l'hébergement d'une application simple à 2 niveaux dans un service à faible code/plateforme. Elle comprend une	• Configuration simple via l'interface utilisateur. • Inclusion des surveillances de l'état, de la mise à l'échelle, de la haute disponibilité. Prise en charge des plateformes, Windows et Linux.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
			base de données relationnelle et une mise à l'échelle automatique pour le niveau application/web.	
Plateforme Opérations 4	Intégration de la sécurité	2	Démonstration des capacités d'intégration de votre plateforme du point de vue de la gestion des incidents et des événements de sécurité.	• Capacité à intégrer et à consommer facilement les journaux relatifs à la sécurité provenant du fournisseur de services cloud + API d'intégration.
Plateforme Opérations 5	Intégration ITSM	3	Démonstration des capacités d'intégration de votre plateforme du point de vue de l'ITSM (gestion des services informatiques).	• Capacité à créer, suivre et mettre à jour un cas d'assistance via une API. • Capacité à allouer des services ou des ensembles de services en tant que « produits » par le biais d'une API.
Plateforme Opérations 6	Support	4	Démonstration de votre offre de prise en charge.	• Différents niveaux de prise en charge pour différents types de charges de travail. • Capacité à prendre également en charge le système d'exploitation, le moteur de base de données, etc., au besoin pour un service donné. • Capacité à proposer une offre en gage de qualité avec des responsables de l'assistance désignés pour les charges de travail critiques. • Capacité à offrir un processus structuré de préparation aux événements et de révision de l'architecture. • Informations sur la feuille de route du fournisseur.
Plateforme Opérations 7	Auditabilité	4	Démonstration de l'outillage dont vous disposez pour soutenir les audits de conformité.	• Capacité à disposer des détails de l'audit de conformité via la console. • Capacité à gérer et automatiser les audits d'environnement.
Plateforme Opérations 8	De la VM au conteneur	1	Démonstration de la conversion d'une application sur une machine virtuelle en un conteneur, et de sa mise en	• Facilité d'utilisation de la conversion. • Temps de conversion. • Prise en charge des plateformes, .Net et Java.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
			service à l'aide de la plateforme de conteneurs du fournisseur de cloud.	

Charge de travail : application web – Exemple d'évaluation technique en temps réel

La section suivante fournit un exemple de feuille d'évaluation de la charge de travail pour une charge de travail « d'application web » spécifique. Lors de l'élaboration d'une fiche d'évaluation pour une application donnée, il est fortement recommandé d'impliquer les utilisateurs, les développeurs et les administrateurs de l'application car ils sont susceptibles de mieux comprendre les exigences, les défis et les contraintes actuels.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
Web Sécurité 1	Sécurité – Protection des applications	3	Démonstration de votre capacité à bloquer les tentatives malveillantes d'exploitation de l'application via l'injection SQL, l'attaque de Scripting XSS etc.	• Capacité à se protéger contre les attaques courantes « prêtes à l'emploi » à l'aide de règles/capacités standard. • Capacité à créer des surveillances/règles/fonctions personnalisées.
Web Sécurité 2	Sécurité – Protection basée sur le débit	3	Démonstration de votre capacité à bloquer/protéger contre les attaques impliquant des taux de requêtes ou des volumes de données importants dirigés vers une application.	• Capacité à configurer des limites et de restreindre les taux de requêtes à partir d'une adresse IP donnée ou d'une liste d'adresses.
Web Sécurité 3	Sécurité – Protection basée sur la source	3	Démonstration de la capacité de restreindre l'accès en fonction du réseau/de la source géographique.	• Capacité de restreindre par bloc de réseau ou par liste de blocs de réseau. • Capacité de restreindre par pays d'origine (sans avoir besoin de gérer des listes IP).

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
Web Sécurité 4	Sécurité – Segmentation du réseau	4	Démonstration de la capacité à isoler/protéger les composants (serveur web, serveur d'applications/serveur de base de données) pour se protéger contre la propagation nord-sud et est-ouest à travers l'infrastructure.	• Capacité à placer des composants dans différents sous-réseaux et de contrôler le flux de trafic entre différents sous-réseaux. • Capacité à contrôler le flux de trafic au niveau de l'interface réseau. • Capacité de référencement des groupes logiques ainsi que des blocs d'adresse CIDR.
Web Sécurité 5	Sécurité – Support TLS et gestion des certificats	4	Démonstration de votre capacité à fournir un point de terminaison sécurisé par TLS et à gérer automatiquement les composants de support pour le fournir, par exemple, la rotation automatique des certificats.	• Prise en charge des derniers protocoles TLS et capacité de désactiver les versions héritées le cas échéant. • Génération, gestion et rotation simples des certificats (idéalement entièrement automatisées).
Web Performance 1	Performances – Capacité de mise à l'échelle	4	Démonstration de votre capacité à changer d'échelle et passer de 10 à 100 000 utilisateurs simultanés de l'application web grâce à la mise à l'échelle automatique dynamique.	• Possibilité de définir des règles de mise à l'échelle basées sur le temps et sur les déclencheurs. • Mise à l'échelle transparente pour l'utilisateur final et l'administrateur. Réduction automatique de l'échelle lorsque la charge augmente et augmentation de l'échelle lorsque la charge diminue. • Assurez-vous que la capacité de mise à l'échelle existe à chaque couche de l'application web (équilibreur de charge, couche web, couche de donnée, etc.). • Disponibilité des services de mise en cache à différentes couches de l'application, le cas échéant.
Web Performance 2	Performance – distribution globale	3	Démonstration de votre capacité CDN, tout en démontrant la latence à partir de différents points du monde, notamment : l'Australie, l'Asie, l'Afrique, le Moyen-Orient, l'Amérique du Nord, l'Amérique du Sud et l'Europe.	• Capacité à créer et de configurer un CDN via la console/les API CISP. • Règles de distribution configurables pour différentes zones géographiques. • Mise en cache configurable pour différents cas d'utilisation/applications.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
Web Fiabilité 1	Fiabilité – Résilience d'une seule région	4	Démonstration de sa capacité à tolérer un événement localisé tel qu'une perte de connectivité réseau au centre de données CISP.	• Basculement automatisé et haute disponibilité dans une région cloud (ville).
Web Fiabilité 2	Fiabilité – Déploiement multirégional	3	Démonstration du déploiement multirégional d'une application web comprenant une base de données répliquée à l'échelle mondiale.	• Capacité à déployer une application multirégion par programmation. • Réplication entre les régions pour le magasin de données. • Routage automatisé des utilisateurs vers leur région optimale.
Web Fiabilité 3	Fiabilité – Basculement multirégional	3	Démonstration du basculement automatique d'une application web en cas de problème de service ayant un impact régional.	• Basculement automatisé et haute disponibilité sur plusieurs régions cloud.
Web Coût 1	Coût – Visibilité	2	Démonstration de sa capacité à suivre le coût par application	• Capacité d'affichage des coûts historiques d'une application spécifique, y compris lorsqu'elle augmente ou baisse
Web Coût 2	Coût – Budgets	2	Démonstration de la capacité à définir des budgets et des alertes associées par application.	• Des budgets configurés par application et la capacité de déclencher des actions/alertes en fonction de seuils configurés.
Web Opérations 1	Ops – Maintenance Windows	3	Démonstration de la capacité à configurer des maintenances Windows en phase avec les besoins de l'entreprise, en particulier lorsque la maintenance peut avoir un impact sur la disponibilité des applications.	• Fenêtres de maintenance configurables pour des composants comme un service de base de données relationnelle.
Web Opérations 2	Ops – Journalisation	3	Démonstration de la capacité à centraliser la journalisation pour une application à plusieurs composants, notamment la persistance des journaux lors de l'arrêt/échec des machines virtuelles.	• Capacité à configurer un service de journalisation centralisé qui peut changer d'échelle en fonction des exigences de l'application. • Capacité à définir des règles/filtres pour déclencher des alertes ou des actions en fonction d'événements du journal spécifiques.

ID du scénario	Nom du scénario	Statut de criticité (1=faible, 4=critique)	Exigences de démonstration	Considérations relatives aux scores
Web Opérations 3	Ops – Surveillance	3	Démonstration de la surveillance de l'application, incluant les performances, la disponibilité, les temps de réponse, le nombre d'erreurs, etc. et la fonctionnalité pour prendre des actions/déclencher des notifications en fonction de différents seuils de métriques.	• Une collection de métriques standard disponibles telles que les E/S de disque, le processeur, les métriques de base de données, le réseau, l'équilibreur de charge, etc. • Capacité à définir des métriques personnalisées ainsi que des seuils. • Capacité à créer un tableau de bord personnalisé pour représenter les métriques les plus importantes et partager ces tableaux de bord avec les utilisateurs concernés.