SERVICES PARTAGÉS CANADA

Invitation à se qualifier pour
Véhicule d'approvisionnement des services infonuagiques du gouvernement du Canada (Infonuagiques GC)

ANNEXE A, APPENDICE 1 – EXIGENCES DE QUALIFICATION POUR LE VOLET 1

Exigence obligatoire	Sous-catégorie	Exigence	Volet 1 – Nécessaires pour démontrer la conformité avec l'exigence en matière d'assurance du palier 2 (incidence moyenne) (données jusqu'au niveau Protégé B inclusivement)
Exigences générales			
O1	Généralités	Le répondant doit indiquer lui-même comme le fournisseur de services d'infonuagique dont les services d'infonuagique disponibles sur le marché seront offerts au gouvernement du Canada à l'étape de l'appel d'offres du présent processus d'approvisionnement.	Déterminer le service d'infonuagique disponible sur le marché proposé : _____ Indiquer le fournisseur de services d'infonuagique pour le service d'infonuagique disponible sur le marché proposé : _____
O2	Généralités	Le fournisseur de services d'infonuagique désigné à l'exigence O1 doit fournir des services d'infonuagique disponibles sur le marché.	Le répondant doit, pour démontrer sa conformité, fournir des documents décrivant les services d'infonuagique disponibles sur le marché proposés figurant dans l'exigence O1. Pour l'exigence O2, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit

			dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O3	Généralités	Les services d'infonuagique disponibles sur le marché proposés doivent permettre au gouvernement du Canada (GC) d'isoler les données au Canada dans un centre de données approuvé. Aux fins de la présente demande de soumissions, un Centre de Données Approuvé satisfait les exigences suivantes : a) Le centre de données doit être situé physiquement au Canada; b) Le centre de données doit répondre aux exigences de sécurité et certifications énoncées au critère O8.	Le répondant doit, pour démontrer sa conformité, fournir des documents illustrant la capacité du service d'infonuagique disponible sur le marché proposé d'isoler les données au Canada dans un centre de données approuvé. Pour être jugés conformes, les documents remis doivent comporter les éléments suivants : a) des captures d'écran du centre de données disponibles dans lesquelles les centres de données canadiens figurent sur la liste de la disponibilité; b) une liste ou une carte indiquant l'emplacement géographique des centres de données au Canada. Pour l'exigence O3, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O4	Généralités	Le fournisseur du service d'infonuagique disponible sur le marché proposé doit pouvoir protéger la confidentialité, l'intégrité et la disponibilité des données des comptes principaux du gouvernement du Canada et des titres de compétences utilisés pour établir l'environnement d'infonuagique du gouvernement du Canada. Il doit aussi s'assurer que les justificatifs d'identité demeurent à l'intérieur des frontières géographiques du Canada.	Le répondant doit, pour démontrer sa conformité, fournir les documents décrivant la capacité du fournisseur de services d'infonuagique à protéger la confidentialité, l'intégrité et la disponibilité des renseignements des comptes principaux du GC, et les justificatifs d'identité utilisés pour établir l'environnement d'infonuagique du GC. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) des documents relatifs au système ou un livre blanc présentant les politiques, les processus et les procédures mis en oeuvre pour protéger la confidentialité, l'intégrité et la disponibilité des renseignements des comptes principaux du gouvernement du Canada , et les titres de compétences utilisés pour établir l'environnement d'infonuagique du gouvernement du Canada. Pour l'exigence O4, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur

			du service d'infonuagique disponible sur le marché proposé satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O5	Généralités	La proposition relative aux services d'infonuagique disponibles sur le marché doit présenter le prix de chacun des services, le mode de facturation et le soutien offert, en dollars canadiens, et, notamment, les rapports de consommation des données.	Le répondant doit, pour démontrer qu'il est en conformité, fournir les documents illustrant la capacité du fournisseur des services d'infonuagique disponibles sur le marché proposés à présenter le prix (en dollars canadiens) des services, le mode de facturation et le soutien, notamment la production de rapports sur la consommation des données. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) des saisies d'écran ou des documents relatifs au système décrivant comment les services seront tarifés, facturés et soutenus, en dollars canadiens. Pour l'exigence O5, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O6	Généralités	Les services d'infonuagique disponibles sur le marché proposés doivent mettre à la disposition de leurs clients les accords sur les niveaux de service (ANS) publiés. Les engagements en matière de niveau de service (précisés dans les accords sur les niveaux de service publiés) doivent offrir aux clients commerciaux un soutien qui comprend, au minimum, le soutien offert sur le marché et rendu public (c.-à-d. la garantie et les services de maintenance et de soutien) généralement fourni aux clients des services d'infonuagique disponibles sur le marché du fournisseur de services d'infonuagique.	Le répondant doit démontrer sa conformité en fournissant des documents qui décrivent les accords sur les niveaux de service publiés du fournisseur de services d'infonuagique et les engagements correspondants pour les services d'infonuagique disponibles sur le marché proposés. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Captures d'écran ou documentation des accords sur les niveaux de service (ANS) publiés détaillant le soutien offert aux clients

			commerciaux sur le marché et rendu public (c.-à-d. la garantie et les services de maintenance et de soutien) généralement fourni aux clients des services d'infonuagique disponibles sur le marché du fournisseur de services d'infonuagique, notamment l'engagement en matière de service, le processus de crédit et le pourcentage de temps de disponibilité.; Pour l'exigence O6, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O7	Généralités	Le fournisseur de services d'infonuagique disponibles sur le marché proposés doit permettre au consommateur de choisir la langue officielle de son choix, soit le français ou l'anglais, quand il navigue sur le site, commande des services au fournisseur de services d'infonuagique et communique avec lui.	Le répondant doit démontrer comment le service d'infonuagique disponible sur le marché proposé permet aux consommateurs de choisir l'une des langues officielles, soit le français ou l'anglais. Pour être jugés conformes, les documents produits doivent démontrer la capacité du service d'infonuagique offert sur le marché à proposer les situations suivantes en français et en anglais : a) parcours des services sur ses sites Web; b) commande des services sur ses sites Web; c) communication avec l'entreprise pour obtenir de l'aide par téléphone, par courriel ou par clavardage. Pour l'exigence O7, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
Exigences liées aux installations des centres de données			

O8	Installations des centres de données	Le fournisseur de services d'infonuagique disponibles sur le marché proposés doit mettre en place des mesures de sécurité qui assurent la protection des installations de technologie de l'information (TI) et des actifs du système d'information dans lesquels les données du gouvernement du Canada sont stockées et protégées contre toute forme de manipulation, de perte, de dommages et de saisie, en fonction d'une approche de sécurité physique axée sur la prévention, la détection, l'intervention et la reprise. Des mesures de protection physique doivent être appliquées conformément aux mesures de contrôle de la sécurité physique, de protection environnementale (PE), de maintenance (MA) et de protection des supports (PS) décrites dans le Profil de contrôle de sécurité pour les services de la TI du GC fondés sur l'infonuagique pour les renseignements classés Protégé B / Intégrité moyenne / Disponibilité moyenne (PBMM) et aux pratiques décrites dans les lignes directrices et normes en matière de sécurité physique de la Gendarmerie royale du Canada (GRC) ou être appliquées selon une approche adéquate axée sur les risques harmonisés à ces mesures et pratiques. Cela comprend au minimum : a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, y compris, être suffisamment disparates sur le plan géographique pour que la perte d'un centre de données n'empêche pas la récupération des données conformément à l'accord sur les niveaux de service (ANS) prescrit; b) l'utilisation adéquate des supports de TI; c) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; d) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; e) la restriction de l'accès physique aux actifs des systèmes d'information aux employés autorisés et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, et validée par deux formes d'identification; f) l'accompagnement des visiteurs et la surveillance des activités des visiteurs; g) la tenue de registres de vérification de l'accès physique; h) le contrôle et la gestion des dispositifs d'accès physique; i) l'application des mesures de protection des données du GC dans les autres lieux de travail (p. ex., lieux de télétravail); j) la consignation et la surveillance de tous les accès physiques aux installations des centres de données et de tous les accès par voie électronique aux composants des systèmes d'information qui hébergent les données du Canada, au moyen d'une combinaison de registres	Le répondant doit démonter comment les services d'infonuagique disponibles sur le marché proposés mettent en place des mesures de sécurité qui assurent la protection des installations de TI et des actifs du système d'information dans lesquels les données du GC sont stockées pour protéger celles-ci contre toute forme de manipulation, de perte, de dommages et de saisie, en fonction d'une approche de sécurité physique axée sur la prévention, la détection, l'intervention et la reprise. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) des documents relatifs au système ou des documents techniques décrivant les politiques, les procédures et les processus utilisés. Pour l'exigence O8, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

		d'accès, de mécanismes de surveillance vidéo dans toutes les zones sensibles et de détection des intrusions.	
Exigences relatives à la sécurité du personnel			
O9	Sécurité du personnel	Le fournisseur des services d'infonuagique disponibles sur le marché proposés doit mettre en place des mesures de sécurité qui accordent et maintiennent le niveau de filtrage de sécurité requis pour le personnel du fournisseur de services d'infonuagique et du sous-traitant en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Les mesures de filtrage doivent être appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115), ou utiliser un équivalent acceptable convenu par le Canada. Cela comprend au minimum : a) une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux données du Canada ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services; b) le processus visant à s'assurer que les employés et les entrepreneurs connaissent, comprennent et respectent leurs responsabilités en matière de sécurité de l'information et que le rôle que l'on compte leur confier leur convient; c) le processus relatif à la sensibilisation et à la formation en matière de sécurité données à l'arrivée des employés et lorsque les rôles des employés et sous-traitants changent; d) le processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi; e) l'approche de détection des personnes malveillantes potentielles à l'intérieur de l'organisation et les mesures de contrôle mises en œuvre pour atténuer le risque d'accès aux données du GC ou les répercussions sur la fiabilité des services d'infonuagique accueillant les actifs et les données du GC.	Le répondant doit démontrer comment les services d'infonuagique disponibles sur le marché proposés mettent en place des mesures de sécurité qui accordent et maintiennent le niveau de filtrage de sécurité requis pour le personnel du fournisseur de services d'infonuagique et du sous-traitant en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) des documents relatifs au système ou des documents techniques décrivant les politiques, les procédures et les processus utilisés. Pour l'exigence O9, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur de services d'infonuagique disponibles sur le marché proposés satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
Exigences liées à l'assurance d'une tierce partie			
O10	Assurance d'une tierce partie	Les services d'infonuagique disponibles sur le marché proposés par le fournisseur services d'infonuagique doivent être conçus et élaborés pour garantir la sécurité des services d'infonuagique disponibles sur le marché proposés et comprendre la mise en œuvre de politiques et de procédures sur la sécurité de l'information et de mesures de contrôle de la sécurité. Le fournisseur de services d'infonuagique qui offre les services d'infonuagique disponibles sur le marché proposés doit aussi respecter les autorisations de sécurité sélectionnées relativement au fournisseur de services d'infonuagique dans le Profil de contrôle de sécurité pour les	Le répondant doit démontrer la façon dont des services d'infonuagique disponibles sur le marché proposés par le fournisseur services d'infonuagique sont conformes à l'exigence O10. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications de l'industrie applicables énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants.

		services de la TI du gouvernement du Canada fondés sur l'informatique en nuage pour les renseignements classés Protégé B/Intégrité moyenne/Disponibilité moyenne (PBMM) en ce qui concerne la portée des services d'infonuagique qu'il offre.	Le répondant doit s'appuyer sur les certifications de l'industrie suivantes pour démontrer sa conformité : a) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences; b) ISO/IEC 27017:2015 Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 des services d'infonuagique; c) Contrôle de l'organisation des services de l'AICPA (SOC) 2 Type II pour les principes de confiance en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité. Chaque certification ou rapport d'évaluation doit : a) indiquer la dénomination sociale du fournisseur de services d'infonuagique proposé; b) indiquer la date ou l'état de la certification actuelle; c) La portée du rapport doit renvoyer aux lieux et aux services proposés par les services d'infonuagique disponibles sur le marché proposés. Si la méthode créée est utilisée pour exclure les organisations de sous-services comme la prise en charge de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être joint; d) être valide pour toute la durée du contrat; e) être délivré par un tiers indépendant certifié en vertu de l'American Institute of Certified Public Accountants (AICPA) ou de CPA Canada (Comptables professionnels agréés du Canada) ou encore du régime de certification ISO, et être conforme à la norme ISO/IEC 17020 sur les systèmes de gestion de la qualité (SGQ); f) avoir été émis au cours des 12 mois précédant la date de clôture de la soumission. Le répondant peut fournir des éléments probants complémentaires tirés de plans de sécurité du système, de l'architecture des systèmes d'information ou de documents permettant de comprendre tout le système, comme une attestation de certification modérée FedRAMP, ou provenant de l'évaluation de ses services selon les critères de la version 3.01 ou ultérieure de Cloud Controls Matrix (CCM) de la Cloud Security Alliance (CSA) pour soutenir les demandes des attestations susmentionnées afin de démontrer la conformité au Profil de contrôle de sécurité pour les services de TI en nuage du gouvernement du Canada des renseignements classés Protégé B/Intégrité moyenne/Disponibilité moyenne (PBMM).
Exigences en matière de protection des données			

O11	Protection des données	Le fournisseur des services d'infonuagique disponibles sur le marché proposés doit permettre au GC de stocker et de protéger ses renseignements inactifs, y compris les données de sauvegarde ou les données tenues à des fins de redondance, à l'intérieur des frontières géographiques du Canada. Cela comprend : a) dresser et fournir au GC une liste à jour des lieux physiques, y compris la ville où pourraient se trouver des données du Canada, au Canada, pour chaque centre de données utilisé pour fournir les services décrits dans ce contrat; b) indiquer les parties des services fournis à partir de l'extérieur du Canada, y compris tous les lieux où les données sont stockées et traitées et où les services sont gérés. c) garantir l'impossibilité de trouver les données d'un client précis sur les supports physiques; d) utiliser le cryptage pour veiller à ce qu'aucune donnée ne soit inscrite sur le disque de manière non cryptée. **Remarque :** Les répondants sont informés que les étapes d'approvisionnement subséquentes peuvent les obliger ou obliger le fournisseur de services d'infonuagique disponibles sur le marché proposés à informer le Canada de toute mise à jour de la liste des lieux physiques où pourraient se trouver des données du Canada.	Le répondant doit fournir les documents démontrant comment le fournisseur des services d'infonuagique disponibles sur le marché proposés (décrits à l'exigence O1) répond à l'exigence obligatoire décrite à l'exigence O11. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) La documentation de système ou la documentation technique précisant et détaillant les politiques, les processus et les procédures servant à stocker et à protéger ses renseignements inactifs, y compris les données de sauvegarde ou les données tenues à des fins de redondance, à l'intérieur des frontières géographiques du Canada; b) Pour les parties des services qui pourraient être offerts depuis l'extérieur du Canada, le répondant doit décrire comment le fournisseur de services d'infonuagique disponibles sur le marché proposés assurera que les données du Canada demeureront protégées contre l'accès, l'utilisation, la divulgation, la modification, l'élimination, la transmission ou la destruction non autorisés. Pour l'exigence O11, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur de services d'infonuagique satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
Exigences en matière de gestion des risques liés à la chaîne d'approvisionnement			
O12	Gestion de la chaîne d'approvisionnement	Le répondant doit fournir une liste de tous les fournisseurs tiers, ainsi que les renseignements portant sur la nature de leur statut (p. ex., filiale, sous-traitant, etc.) qui fourniraient au Canada des services d'infonuagique disponibles sur le marché proposés. Pour les besoins de cette exigence, une entreprise qui fournit des biens au fournisseur de services d'infonuagique disponibles sur le marché proposés, mais qui n'effectue pas une partie de la chaîne d'approvisionnement qui	Le répondant doit fournir des documents qui présentent des renseignements sur tous les tiers auxquels on pourrait faire appel pour effectuer une partie quelconque de la chaîne d'approvisionnement en mesure de fournir au Canada des services d'infonuagique disponibles sur le marché proposés, qu'il s'agisse : (i) de sous-traitants du répondant ou du fournisseur de services d'infonuagique; (ii) de sous-traitants des sous-traitants du répondant ou du fournisseur de services d'infonuagique, en aval;

		pourrait fournir au Canada des services d'infonuagique disponibles sur le marché proposés, n'est pas considérée comme un tiers. Les tiers peuvent comprendre, par exemple, les techniciens qui pourraient être déployés ou qui entretiennent les services d'infonuagique disponibles sur le marché du fournisseur de services d'infonuagique qui ont été proposés par le répondant à l'exigence O1. **Remarque :** Les répondants sont informés que les étapes d'approvisionnement subséquentes peuvent les obliger à informer régulièrement le Canada de toute mise à jour de la liste de fournisseurs tiers.	(iii) de toute filiale. La liste doit au moins comporter ce qui suit : a) le nom du tiers; b) l'adresse du siège social du tiers; c) la portion des travaux qui serait exécutée par le tiers; d) les emplacements où le tiers fournirait au Canada les services d'infonuagique disponibles sur le marché proposés; e) tout tiers qui pourrait avoir accès aux données du Canada dans le cadre des services d'infonuagique disponibles sur le marché proposés. Si le fournisseur de services d'infonuagique ne fait appel à aucun tiers pour effectuer une partie quelconque de la chaîne d'approvisionnement en mesure de fournir au Canada des services d'infonuagique disponibles sur le marché proposés, le répondant doit l'indiquer dans sa réponse à cette exigence.
O13	Gestion des risques liés à la chaîne d'approvisionnement	Le fournisseur de services d'infonuagique des services d'infonuagique disponibles sur le marché proposés doit prendre des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services. Ces mesures comprennent, sans s'y limiter, la conception et la mise en œuvre de mesures de contrôle visant à atténuer et à contenir les risques liés à la sécurité des données au moyen de la répartition convenable des tâches, de l'accès reposant sur le rôle et des droits d'accès minimaux pour tout le personnel au sein de la chaîne d'approvisionnement.	Le répondant doit démontrer la façon dont des services d'infonuagique disponibles sur le marché proposés par le fournisseur services d'infonuagique sont conformes à l'exigence O13. Pour être jugés conformes, les documents fournis doivent démontrer que la démarche de gestion des risques de la chaîne d'approvisionnement du fournisseur de services d'infonuagique respecte l'une des pratiques exemplaires suivantes et qu'elle est évaluée et validée par un tiers indépendant certifié en vertu de l'AICPA ou du CPA du Canada ou encore du régime de certification ISO : 1. ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4); **OU** 2. NIST Special Publication 800-161 – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*; **OU** 3. Catalogue des contrôles de sécurité ITSG-33, sections SA-12 et SA-12(2) où les mesures de sécurité établies et structurées sont décrites dans un plan de Gestion des risques de la chaîne d'approvisionnement (GRCA). Le plan GRCA doit décrire la démarche du fournisseur de services d'infonuagique en matière de GRCA et démontrer comment le fournisseur de services d'infonuagique disponibles sur le marché proposés réduira et atténuera les risques associés à la chaîne d'approvisionnement.

Exigences relatives à la protection des renseignements personnels			
O14	Protection des renseignements personnels	Le fournisseur de services d'infonuagique disponibles sur le marché proposés doit démontrer qu'il respecte les politiques, procédures et dispositions de confidentialité qui satisfont aux certifications de l'industrie suivantes : a) ISO/IEC 27018:2014 Technologies de l'information – Techniques de sécurité – Code de pratique pour la protection des informations personnelles identifiables (PII) dans les nuages publics agissant en tant que processeurs PII. **Remarque :** Les répondants sont informés que les étapes d'approvisionnement subséquentes peuvent les obliger de confirmer régulièrement au Canada que les services d'infonuagique disponibles sur le marché proposés respectent la certification ci-dessus et que la certification est valide pour toute la durée du contrat.	Pour démontrer sa conformité à la certification, le répondant doit fournir : a) une copie des documents de certification ISO 27018 les plus récents du fournisseur de services d'infonuagique, qui doivent avoir été délivrés dans les 12 mois précédant la date de clôture des demandes de soumissions; b) une copie du rapport d'évaluation ISO 27018 de ses services d'infonuagique commerciaux actuellement offerts.