APPENDICE M – EXIGENCES RELATIFS A LA SÉCURITÉ NIVEAU 2

Exigences relatives à la sécurité pour logiciel-service

Exigences de qualification

Les vingt (20) exigences de sécurité suivantes doivent être satisfaites afin de démontrer la conformité à l'assurance du palier 2 **(données jusqu'au niveau Protégé B inclusivement).**

2. <u>Palier 2 (Renseignements classifiés jusqu'à la catégorie Protégé B inclusivement)</u>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O1.	Rôles et responsabilités en matière de sécurité	Le fournisseur doit définir clairement les rôles et les responsabilités en ce qui concerne les contrôles de sécurité et les fonctionnalités des services entre le fournisseur (tout sous-processeur du fournisseur, le cas échéant) et le Canada.	Dans le document, le fournisseur doit inclure, au minimum, les rôles et responsabilités des parties en ce qui concerne: (i) la gestion des comptes; (ii) la protection des frontières; (iii) la sauvegarde des actifs et du système d'information; (iv) la gestion des incidents; (v) la surveillance du système; et (vi) la gestion des vulnérabilités.
O2.	Gestion des comptes principaux/racines	Le fournisseur de logiciels-services commercialement disponible 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. Cela comprend l'assurance que les justificatifs d'identité restent à l'intérieur des frontières géographiques du Canada.	Le fournisseur doit démontrer sa conformité en fournissant de la documentation qui décrit la capacité du logiciel-service commercialement disponible de protéger la confidentialité, l'intégrité et la disponibilité de l'information et des justificatifs d'identité du compte principal du gouvernement du Canada (GC) utilisés pour établir l'environnement infonuagique du GC. 1) Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Documentation du système ou livre blanc décrivant les politiques, les processus et les procédures utilisés pour protéger la confidentialité, l'intégrité et la disponibilité de l'information et des justificatifs d'identité du compte principal du GC utilisés pour établir l'environnement infonuagique du

			GC. a) Pour les exigences, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercialement disponible proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer où trouver le matériel

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
			de référence dans la réponse, y compris le titre du document, ainsi que les numéros de page et de paragraphe. c) Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur 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	Isolation de la protection des données	Les services proposés doivent permettre au 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 est défini comme suit : a) un centre de données situé physiquement au Canada; b) un centre de données qui répond à toutes les exigences de sécurité et certifications énoncées dans les exigences relatives aux installations des centres de données. Exigences relatives aux installations des centres de données: Le fournisseur du logiciel-service commercialement disponible proposé doit veiller à mettre en œuvre des mesures de sécurité qui assurent la protection des installations de TI et des actifs du système d'information dans lesquels les données du Canada sont stockées et traitées 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 physiques doivent être appliquées conformément aux mesures de contrôle de la protection physique et environnementale (PE), de la maintenance (MA) et de la protection des supports (PS) décrits dans les contrôles de sécurité décrits dans ITSG-33 Profil de contrôle de sécurité du gouvernement du Canada pour les services de TI du GC en nuage pour « PBMM » et aux pratiques décrites dans les lignes directrices et normes en matière de sécurité physique de la Gendarmerie royale du Canada (GRC). Cela comprend au minimum :	Le fournisseur doit fournir une documentation qui démontre comment le fournisseur des services proposés se conforme aux exigences énoncées à la rubrique Exigences relatives aux installations des centres de données. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la protection des installations de TI et des actifs du système d'information dans lesquels les données du GC sont stockées et traitées 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 les exigences relatives aux installations des centres de données, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le logiciel-service commercialement disponible satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer où trouver le matériel de référence dans la réponse, y compris le titre du document, ainsi que les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont notamment 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'ENS prescrite; d) l'utilisation adéquate des supports de TI; b) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; e) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; f) 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, validé par deux formes d'identification; g) l'escorte des visiteurs et la surveillance de leurs activités; h) la tenue de registres de vérification de l'accès physique; i) le contrôle et la gestion des dispositifs d'accès physique; j) l'application de mesures de protection des données du Canada à d'autres lieux de travail (p. ex., les sites de télétravail); b) 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 d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.	
O4	Séparation des données	Le fournisseur doit, pour les deux tiers, mettre en place des contrôles pour assurer l'isolation appropriée des ressources, de sorte que les actifs informationnels ne soient pas mélangés avec les données d'autres locataires, qu'ils soient en cours d'utilisation, de stockage ou de transit, ainsi que dans tous les aspects des fonctionnalités du service fournisseur et de l'infrastructure fournisseur. et administration du système. Cela inclut la mise en œuvre de contrôles d'accès et l'application de la séparation logique ou physique appropriée pour prendre en charge:	Le fournisseur doit fournir une documentation démontrant que le fournisseur des services proposés se conforme aux exigences.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		(a) la séparation entre l'administration interne du fournisseur et les ressources utilisées par ses clients; et ( ) La séparation des ressources du client dans des environnements multi-locataires afin d'empêcher qu'un consommateur malveillant ou compromis affecte le service ou les données d'un autre.	
O5	Protection des données	Le fournisseur du logiciel-service commercialement disponible proposé 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 les éléments suivants : 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 des services; b) indiquer les parties des services fournis à partir de l'extérieur du Canada, y compris tous les lieux oil les données sont stockées et traitées et où les services sont gérés; b) garantir l'impossibilité de trouver les données d'un client précis sur les supports physiques; c) utiliser le cryptage pour veiller à ce qu'aucune donnée ne soit inscrite sur le disque de manière non cryptée. Remarque à l'attention des fournisseurs : Les fournisseurs sont informés que les étapes d'approvisionnement subséquentes peuvent les obliger ou obliger le fournisseur du logiciel-service commercialement disponible proposé à informer le Canada de toute mise à jour de la liste des lieux physiques où pourraient se trouver des données du Canada	Le fournisseur doit, pour démontrer sa conformité, fournir des documents illustrant la capacité du logiciel-service commercialement disponible proposé d'isoler les données au Canada dans un centre de données approuvé. Pour être jugés conformes, les documents 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 ce critère, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le logiciel sous forme de service commercialement disponible proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur 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	Installations des centres de données	Le fournisseur du logiciel-service commercialement disponible proposé doit veiller à mettre en œuvre 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 et traitées 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,	Le fournisseur doit fournir une documentation qui démontre comment le fournisseur des services proposés se conforme aux exigences énoncées à la rubrique Exigences relatives aux installations des centres de données. Pour être jugés conformes, les documents doivent comporter les éléments suivants :

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2

		l'intervention et la reprise. Les mesures de protection physique doivent être appliquées en conformité avec, ou utiliser une approche adéquate, basée sur les risques et alignée sur les conditions physiques, alignées sur les contrôles de sécurité physique et les pratiques du Conseil du Trésor sur la sécurité physique (http: //www.tbs- sct.gc.ca/pol/doc-fra.aspx?id=12329). Les mesures de sécurité requises à cet égard comprennent, au minimum; a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont notamment 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'ENS prescrite; k) l'utilisation adéquate des supports de TI; l) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; c) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; d) 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, validé par deux formes d'identification; e) l'escorte des visiteurs et la surveillance de leurs activités; b) la tenue de registres de vérification de l'accès physique; f) le contrôle et la gestion des dispositifs d'accès physique; g) l'application de mesures de protection des données du GC à d'autres lieux de travail (p. ex., les sites de télétravail); c) 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 d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.	a) une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la protection des installations de TI et des actifs du système d'information dans lesquels les données du Canada sont stockées et traitées 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 les exigences relatives aux installations des centres de données, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le logiciel sous forme de service commercialement disponible satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O7	Sécurité du personnel	Le fournisseur du logiciel-service commercialement disponible proposé 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 en matière de filtrage de sécurité 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; m) 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; b) 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; n) le processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi; o) l'approche de détection des initiés malveillants potentiels et les contrôles mis en œuvre pour atténuer le risque d'accès aux données du GC ou de dommage à la fiabilité des services d'infonuagique hébergeant les actifs et données du GC.	Le fournisseur doit fournir une documentation qui démontre comment le fournisseur des services proposés se conforme aux exigences énoncées à la rubrique Exigences de sécurité du personnel. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) la documentation du système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, les processus et les procédures qui sont utilisés pour accorder et maintenir le niveau requis de vérification de sécurité pour le fournisseur et le personnel des sous-traitants conformément à leurs privilèges d'accès aux biens du système d'information dans lesquels les données du Canada sont stockées et traitées. Pour les exigences de sécurité du personnel, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercialement disponible proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer où trouver le matériel de référence dans la réponse, y compris le titre du document, ainsi que les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur 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.
O8	Assurance d'une tierce partie	Le logiciel sous forme de service commercialement disponible doit être conçu et élaboré pour garantir la sécurité du logiciel-service commercialement disponible proposé 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 du logiciel-service commercialement disponible proposé doit également se conformer aux exigences de sécurité sélectionnées dans le Profil des mesures de sécurité pour les	Le fournisseur doit démontrer comment le fournisseur du logiciel-service commercialement disponible proposé se conforme aux exigences de la rubrique Exigences relatives à l'assurance des tiers. 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		services de la TI du GC fondés sur l'informatique en nuage les renseignements classés « Protégés B, intégrité moyenne, disponibilité moyenne » (PBMM) pour la portée du logiciel-service commercialement disponible proposé fourni. La conformité sera validée et vérifiée par le biais du processus d'évaluation du Centre canadien de cyber sécurité (CCCS), du fournisseur de services cloud (CSP), de la sécurité des technologies de l'information (TI) (ITSM.50.100) (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux). Tout fournisseur ayant participé au processus doit fournir une documentation confirmant qu'il a terminé le processus d'intégration avec (i) une copie du rapport d'évaluation complété le plus récent fourni par CCCS; et (ii) une copie du dernier rapport de synthèse fourni par CCCS. Cela accélérera le processus de qualification et ne demandera pas au fournisseur de démontrer la conformité Pour lancer le processus d'intégration, le fournisseur doit contacter le service clientèle de CCCS pour recevoir une copie du formulaire de soumission d'intégration, ainsi que toute information supplémentaire relative au programme d'évaluation informatique du CSP.	Le fournisseur doit fournir chacune des certifications suivantes de l'industrie pour démontrer sa conformité : 1) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences 0) 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 pour les services du nuage 2) AICPA Service Organisation Control (SOC) 2 de type II pour les principes de confiance de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité. Chaque certification ou rapport d'évaluation doit : a) être valide à la date de clôture de la demande de soumissions; d) indiquer la raison sociale légale du fournisseur du logiciel-service commercialement disponible proposé et du fournisseur de services d'informatique en nuage; b) indiquer la date ou l'état de la certification actuelle; p) donner la liste des actifs, de l'infrastructure du fournisseur et emplacements de service dans le cadre du rapport de certification; c) la portée du rapport doit renvoyer aux lieux et aux services proposés par le logiciel sous forme de service commercialement disponible proposé. 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; et d) 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. Le fournisseur peut fournir des renseignements supplémentaires tirés de plans de sécurité du système, de documents de conception de système d'information, de documents d'architecture de système d'information ou de documents qui donnent une description détaillée du système, comme l'évaluation de ses services conformément à la version 3.01 de la Cloud Controls Matrix (CCM) de la Cloud Security Alliance (CSA) ou à une version subséquente, pour complémenter les allégations de certifications ci-dessus, afin de démontrer la conformité au Profil des mesures de sécurité pour les services de la TI du GC

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
			fondés sur l'informatique en nuage pour les renseignements classés Protégé B, intégrité moyenne et disponibilité moyenne (PBMM). Remarque : • Des certifications doivent être fournies pour toutes les parties des services proposés. • Les certifications doivent être accompagnées de rapports d'évaluation.
O9	Programme d'évaluation de la sécurité des TI	Le fournisseur doit démontrer qu'il se conforme aux exigences de sécurité choisies dans le Profil des mesures de sécurité pour les services de TI du GC fondés sur l'informatique en nuage (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) pour la portée des services fournis par le fournisseur dans le cadre du Programme d'évaluation de la sécurité des TI.	Le fournisseur doit démontrer qu'il se conforme aux exigences de sécurité choisies dans le Profil des mesures de sécurité pour les services de TI du GC fondés sur l'informatique en nuage (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) pour la portée des services fournis par le fournisseur dans le cadre du Programme d'évaluation de la sécurité des TI. 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. La mise en correspondance des mesures de sécurité doit inclure : le Profil des mesures de sécurité pour les services de TI du GC fondés sur l'informatique en nuage; la certification de l'industrie en matière d'assurance par un tiers; la mise en correspondance entre le Profil des mesures de sécurité pour les services de TI du GC fondés sur l'informatique en nuage et la certification de l'industrie en matière d'assurance de tiers.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O10	Gestion de la chaîne d'approvisionnement	Le fournisseur doit fournir une liste de fournisseurs tiers contenant des renseignements sur tout tiers (p. ex. filiales, sous-traitants, etc.) qui fournirait au Canada le logiciel sous forme de service commercialement disponible. Pour les besoins de cette exigence, une entreprise qui fournit des biens au fournisseur du logiciel-service commercialement disponible proposé, mais qui n'effectue pas une partie de la chaîne d'approvisionnement qui pourrait fournir au Canada le logiciel sous forme de service commercialement disponible proposé, n'est pas considérée comme un tiers. Les exemples de tiers comprennent, par exemple, les techniciens qui pourraient être déployés ou entretenir le logiciel sous forme de service commercialement disponible proposé par le fournisseur dans les exigences générales. Remarque : Les fournisseurs sont informés que les étapes d'approvisionnement subséquentes peuvent exiger que le fournisseur avise périodiquement le Canada en cas de mise à jour de la liste des fournisseurs tiers.	Le fournisseur 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 un logiciel sous forme de service commercialement disponible proposé, qu'il s'agisse : (i) des sous-traitants du fournisseur; ( )des sous-traitants de sous-traitants du fournisseur en aval de la chaîne; iii) toute filiale. Le fournisseur doit remplir le formulaire 6 - Modèle de soumission SCI tel que fourni dans la présente DAMA. Si le fournisseur ne fait pas appel à des tiers pour effectuer une partie de la chaîne d'approvisionnement susceptible de fournir au Canada le logiciel-service proposé disponible dans le commerce proposé, il est demandé au fournisseur de l'indiquer dans sa réponse à cette exigence. Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O11	Gestion des risques de la chaîne d'approvisionnement	Le fournisseur du logiciel-service commercialement disponible proposé 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. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.	Le fournisseur doit démontrer en quoi le fournisseur du logiciel disponible dans le commerce proposé en tant que service est conforme aux exigences des exigences de gestion des risques de la chaîne logistique décrites dans le programme d'évaluation de la sécurité des technologies de l'information des fournisseurs. Pour être considérée comme conforme, la documentation fournie doit démontrer que l'approche de gestion des risques de la chaîne d'approvisionnement utilisée dans le commerce comme logiciel disponible dans le commerce s'aligne sur l'une des meilleures pratiques suivantes. 1. ISO / CEI 27036 Technologies de l'information - Techniques de sécurité - Sécurité de l'information pour les relations avec les fournisseurs (parties 1 à 4); ou 2. Publication spéciale NIST 800-161 - Pratiques de gestion des risques de la chaîne d'approvisionnement pour les systèmes et organisations d'information fédéraux; ou 3. Contrôle de sécurité ITSG-33 pour SA-12 et SA-12 (2) lorsque les garanties de sécurité définies sont documentées dans un plan de gestion des risques liés à la chaîne logistique. Le plan de SCRM doit décrire l'approche du fournisseur en matière de SCRM et indiquer comment les fournisseurs du logiciel-service proposé dans le commerce proposé réduiront et atténueront les risques inhérents à la chaîne d'approvisionnement. Le plan SCRM doit être évalué et validé de manière indépendante par un tiers indépendant certifié selon le régime de certification AICPA ou CPA Canada et / ou ISO. Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O12	Confidentialité	Le fournisseur de logicies-services commercialement disponible proposé doit démontrer qu'il est conforme aux règles, procédures et dispositions relatives à la confidentialité, qui répondent aux exigences de la certification de l'industrie suivante: 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 fournisseurs sont informés que les phases d'approvisionnement ultérieures peuvent obliger le fournisseur à confirmer régulièrement au Canada de logicies-services commercialement disponible répond à la certification ci-dessus et que cette certification est valide pour toute la durée du véhicule d'approvisionnement.	Pour démontrer la conformité à la certification, le fournisseur doit fournir: a) Une copie des documents de certification de logicies-services commercialement disponible les plus récents, ainsi que des documents de certification ISO 27018, qui doivent avoir été délivrés au plus tard 12 mois avant la date de clôture de la soumission; et b) Une copie du rapport d'évaluation ISO 27018 de logicies-services commercialement disponible et de services et de services cloud. Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2

O13	Confidentialité par conception	Le fournisseur doit démontrer qu'il: a) met en œuvre un cycle de vie de développement logiciel conforme à la norme ISO 27032 et et met en œuvre la confidentialité par la conception ; c) est conforme au cadre de gestion de la confidentialité et aux exigences de la politique spécifiées dans la norme ISO 29100; et d) Adhère à la confidentialité dès la conception des 7 principes fondamentaux (voir https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).	Le fournisseur doit fournir une documentation démontrant que le fournisseur des services proposés se conforme aux exigences. Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O14	Gestion d'accès privilégié	Le fournisseur du logiciel-service commercialement disponible proposé doit fournir une documentation de système démontrant comment le logiciel sous forme de service est en mesure de répondre aux exigences de sécurité suivantes en matière de gestion d'accès privilégié : a) gérer et surveiller l'accès privilégié aux services d'infonuagique pour s'assurer que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC; b) restreindre et réduire au minimum l'accès aux services et aux actifs d'information du Canada aux seuls dispositifs autorisés et aux utilisateurs finaux ayant un besoin explicite d'y avoir accès; e) exécuter et vérifier les autorisations d'accès aux services et aux actifs d'information; f) limiter tous les accès aux interfaces de service qui hébergent les actifs et les actifs d'information aux utilisateurs finaux, dispositifs et processus (ou services) désignés, authentifiés et autorisés de façon unique; c) mettre en œuvre des politiques relatives aux mots de passe afin de protéger les justificatifs d'identité contre les attaques en ligne ou hors ligne et de détecter ces attaques en enregistrant et en surveillant des événements tels que (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle de ces justificatifs et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément au document ITSP.30.031 V2 (ou versions ultérieures) (https://www.cse-cst.gc.ca/fr/node/1842/html/26717) du CST; d) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier (palier 2 seulement) les utilisateurs finaux ayant un accès privilégié, conformément au document ITSP.30.031 V2 (ou versions ultérieures) du CST (https://www.cse-cst.gc.ca/fr/node/1842/html/26717); e) mettre en place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux actifs et aux actifs d'information;	Le fournisseur doit démontrer sa conformité en fournissant de la documentation qui décrit la capacité du logiciel-service commercialement disponible de répondre aux exigences de sécurité liées aux exigences en matière de gestion de l'accès privilégié : Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) une documentation du système ou un livre blanc décrivant les politiques, les processus et les procédures utilisés pour prendre en charge la gestion de l'accès privilégié. Pour la gestion de l'accès privilégié, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercialement disponible proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		h) définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, les rôles de développement des rôles opérationnels et les rôles de gestion de l'accès des autres rôles opérationnels; i) adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services et actifs et aux actifs d'information; j) mettre en place des contrôles d'accès aux objets stockés et des politiques d'autorisation granulaires pour autoriser ou limiter l'accès; k) utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (par exemple un point terminal dédié qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) pour offrir le soutien et l'administration des services et de l'infrastructure; l) mettre en place un processus automatisé pour effectuer une vérification périodique de la création, de la modification, de l'activation, de la désactivation et de la suppression de comptes; et) révoquer, en cas de cessation d'emploi, les authentifiants et les justificatifs d'accès associés au personnel chargé des services.	

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 1
O15	Fédération de l'identité	**Fédération de l'identité** Le fournisseur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment : a) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://cyber.gc.ca/fr/node/1842/html/26717); b) prendre en charge le Security Assertion Markup Language (SAML) 2.0 et OpenID Connect 1.0, où les justificatifs et authentificateurs des utilisateurs finaux pour les services d'infonuagique sont contrôlés uniquement par le Canada; c) permettre d'associer les identifiants uniques du Canada (p. ex. un numéro d'identification unique du Canada, une adresse de courriel du Canada) aux comptes d'utilisateurs des services d'infonuagique correspondants.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fédération de l'identité. Pour être jugée conforme, la documentation fournie doit inclure : a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Fédération de l'identité, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O16	Protection des points d'extrémité	**Protection des points d'extrémité** Le fournisseur doit mettre en œuvre, gérer et surveiller les points d'accès sécurisés afin de prévenir les attaques et les abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide to General Server Security [guide relatif à la sécurité générale des serveurs]), des points de référence du Center for Internet Security (CIS) ou d'une norme équivalente approuvée par écrit par le Canada.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection des points d'extrémité. Pour être jugée conforme, la documentation fournie doit inclure : b) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Protection des points d'extrémité, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 1
			documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O17	Développement sécurisé	**Développement sécurisé** Le fournisseur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : i) NIST, ii) ISO, iii) ITSG-33, iv) SAFECode ou v) Open Web Application Security Project (OWASP) (p. ex. Application Security Verification Standard [ASVS]) ou une norme équivalente approuvée par le Canada par écrit.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Développement sécurisé. Pour être jugée conforme, la documentation fournie doit inclure : c) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Développement sécurisé, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O18	Gestion à distance du fournisseur	**Gestion à distance des fournisseurs** Le fournisseur doit gérer et surveiller l'administration à distance du service du fournisseur utilisé pour héberger les services du GC et prendre des mesures raisonnables pour: (a) Mettre en œuvre des mécanismes d'authentification multi-facteurs pour authentifier les utilisateurs d'accès distant,	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Gestion à distance du fournisseur. Pour être jugée conforme, la documentation fournie doit inclure : a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 1
		conformément au ITSP.30.031 V2 du CST (ou versions ultérieures) (https://www.cse-cst.gc.ca/fr/node/1842/html / 26717); (b) Employer un algorithme cryptographique approuvé par le CSTC pour protéger la confidentialité des sessions d'accès à distance; (c) acheminez tous les accès à distance via des points de contrôle d'accès contrôlés, surveillés et vérifiés; (d) déconnecter ou désactiver rapidement les connexions de gestion à distance ou d'accès à distance non autorisées; (e) Autoriser l'exécution à distance de commandes privilégiées et l'accès à distance aux informations relatives à la sécurité.	politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections de la Gestion à distance du fournisseur, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O19	Fuite d'information	**Fuite d'information** a) Le fournisseur doit fournir au Canada un document décrivant le processus qu'il suit pour répondre à un incident de fuite d'information. Le processus du fournisseur doit être harmonisé i) aux directives de la section IR-9 intitulée « Intervention en cas de fuite d'information » du document ITSG-33, ou b) ii) à une autre pratique exemplaire des principaux fournisseurs de services approuvée par écrit par le Canada. Nonobstant ce qui précède, le processus d'intervention en cas de fuite d'information du fournisseur doit comprendre, à tout le moins : b) un processus d'identification du renseignement précis impliqué dans la contamination d'un actif ou d'un système; c) un processus visant à isoler et à éradiquer un renseignement ou un système contaminé; d) un processus d'identification des renseignements ou des systèmes pouvant avoir été subséquemment contaminés et de toute autre mesure prise pour empêcher la propagation de la contamination. c) Le fournisseur doit transmettre au Canada un processus d'intervention en cas de fuite d'information à jour, et ce, chaque année ou après toute modification apportée au processus de gestion de ces incidents.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fuite d'information. Pour être jugée conforme, la documentation fournie doit inclure : b) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Fuite d'information, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 1
O20	Protection Cryotographique	**Protection cryptographique** Le fournisseur doit fournir au Canada un document décrivant le processus suivi pour répondre à une protection cryptographique de l'information. e) Configurez toute cryptographie utilisée pour mettre en œuvre des sauvegardes de confidentialité ou d'intégrité, ou utilisée dans le cadre d'un mécanisme d'authentification (solutions VPN, TLS, modules logiciels, infrastructure à clé publique et jetons d'authentification, le cas échéant), conformément au Centre de la sécurité des communications (CST). - algorithmes cryptographiques, tailles de clés cryptographiques et périodes cryptographiques approuvés; g) Utilisez des algorithmes cryptographiques, des tailles de clés cryptographiques et des périodes cryptographiques validées par le programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/), et spécifiés dans ITSP.40.111 Algorithmes cryptographiques. pour les informations non classifiées, protégées A et protégées B, ou des versions ultérieures (https://cyber.gc.ca/fr/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111); h) Assurez-vous que la cryptographie validée FIPS 140 est utilisée lorsque le cryptage est requis, et qu'elle est implémentée, configurée et utilisée dans un module cryptographique, validée par le programme de validation du module cryptographique (https://www.cse-cst.gc.ca/ programme de validation module / crypto-module), dans un mode approuvé ou autorisé, afin de fournir un degré élevé de certitude que le module cryptographique validé FIPS 140-2 fournit les services de sécurité attendus de la manière attendue; et i) Assurez-vous que tous les modules FIPS 140-2 utilisés possèdent une certification active, à jour et valide. Les produits conformes / validés FIPS 140 auront des numéros de certificat	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection Cryptographique. Pour être jugée conforme, la documentation fournie doit inclure : c) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections de la Protection Cryptographique, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.