RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Quebec
K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

Title - Sujet
IQ – SGIPAE pour Santé Canada

Solicitation No. - N° de l'invitation	**Date**
HT300-193651/A	2020-05-08

Client Reference No. - N° de référence du client
HT300-193651

GETS Reference No. - N° de référence de SEAG
PW-$EEM-052-37776

File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
052eem.HT300-193651	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2020-06-05

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Nkiama, Ngoma	052eem

Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 850-1643 ( )	(819) 956-2675

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Specified Herein
Précisé dans les présentes

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
See Herein	

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Issuing Office - Bureau de distribution

Mainframe & Business Software Procurement Division / Div des achats des ordi principaux et des logiciels de gestion
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Quebec
K1A 0S5

INVITATION À SE QUALIFIER (IQ)

POUR LE

SYSTÈME DE GESTION DE L'INFORMATION DU PROGRAMME D'AIDE AUX EMPLOYÉS (SGIPAE)

DE

SANTÉ CANADA

AVIS IMPORTANT :

CE DOCUMENT CONTIENT UNE EXIGENCE EN MATIÈRE DE SÉCURITÉ

TABLE DE MATIÈRE

LISTE DES ANNEXES

LISTE DES FORMULAIRES

PARTIE 1 : RENSEIGNEMENT GÉNÉRAUX

1.1 Introduction

La présente Invitation à se qualifier (IQ) compte cinq parties, ainsi que des annexes et elle est divisée comme suit :

Partie 1 Renseignements généraux renferment les instructions, les clauses et les conditions relatives à l'étape de l'IQ.

Partie 2 Instructions à l'intention des répondants : renferme les instructions des clauses et conditions relatives à l'étape de l'IQ.

Partie 3 Instructions pour la préparation des réponses : renferme les consignes aux répondants sur la façon de préparer leur réponse à l'IQ et ainsi que les critères d'évaluation à rencontrer.

Partie 4 Procédures d'évaluation et sélection des répondants retenus : décrit la façon selon laquelle se déroulera l'évaluation des réponses et la méthode de sélection des répondants retenus.

Partie 5 Attestations : comprend les attestations à fournir dans la réponse, des attestations additionnelles peuvent être incluses dans la Demande de soumissions (DDS), s'il y a lieu.

1.2 Résumé

(a) La présente invitation à se qualifier (IQ) est émise par le Canada à l'égard du projet généralement décrit à la section 1.3 ci-dessous pour la fourniture du Système de gestion de l'information du Programme d'aide aux employés (SGIPAE) pour Santé Canada. La division des Services d'aide aux employés (SAE) de Santé Canada a, par décret, reçu le mandat de fournir le Programme d'aide aux employés (PAE) et les services connexes aux organismes publics fédéraux, aux ministères et aux organismes sous réglementation fédérale.

(b) Le but de cette IQ est d'inviter les parties intéressées à soumettre une réponse indiquant leur intérêt et leurs qualifications pour le projet. Sur la base de ces réponses, le Canada a l'intention de sélectionner, conformément aux modalités de la présente IQ, une liste d'un maximum de huit (8) répondants qualifiés pour participer aux phases subséquentes du processus d'approvisionnement, à savoir la phase de l'examen et amélioration des exigences (EAE) et la phase de Demande de soumissions (DDS) pour la sélection d'un seul entrepreneur pour fournir le SGIPAE requis.

(c) Dans la présente IQ, sauf dans la mesure où le contexte ou les dispositions expresses de cette IQ l'exigent par ailleurs, tout mot ou terme en majuscule non autrement défini dans les instructions du répondant à l'IQ a le sens qui lui est attribué à l'annexe A - Définitions et interprétation.

(d) Toute partie intéressée peut soumettre une réponse. Les répondants peuvent être des personnes physiques, des sociétés, des coentreprises/consortiums, des partenariats ou toute autre entité juridique.

(e) Aucune autorisation de sécurité n'est requise pour participer à cette IQ. L'annexe D – Ébauche d'exigences relative à la sécurité applicables aux solutions sur site à l'étape de la DDS, l'annexe E - Liste de vérification des exigences relatives à la sécurité (LVERS) et l'annexe F - Ébauche des exigences relatives à la sécurité applicables aux solutions de logiciels-services à l'étape de la DDS décrivent les exigences de sécurité obligatoires essentielles applicables à l'étape de la DDS. Ces exigences décrivent certaines, mais pas nécessairement toutes les exigences que le Canada a l'intention de traiter dans la DDS. Des

exigences relatives à la sécurité supplémentaires peuvent être incluses dans les phases ultérieures de ce processus d'approvisionnement. Le Canada inclut ces exigences dans la présente IQ afin d'informer les répondants à l'avance de certaines des exigences susceptibles d'être incluses dans la DDS connexe.

(f) En raison du temps qu'il faut pour obtenir ces autorisations de sécurité, les répondants potentiels sont fortement encouragés à amorcer le processus d'habilitation de sécurité et à soumettre à l'autorité contractante les documents requis le plus tôt possible au cours de l'étape de l'IQ. Les documents incomplets ou incorrectement remplis constituent une raison courante de retard dans l'autorisation, car on encourage les répondants éventuels à vérifier soigneusement les documents avant de les soumettre.

(g) La présente IQ ne constitue pas une demande de soumissions ou un appel d'offres. Elle vise uniquement à pré-qualifier des Répondants. Aucun contrat ne résultera de cette IQ. Cette IQ peut en tout temps être partiellement ou complètement annulée par le Canada. Par conséquent, il n'y a aucune garantie qu'une étape d'approvisionnement suivra l'étape d'IQ. Le Canada se réserve le droit d'annuler toute exigence préliminaire faisant partie du projet à tout moment pendant l'étape de l'invitation à se qualifier ou à toute autre étape du processus d'approvisionnement. Étant donné qu'il ne s'agit pas d'un appel d'offre, les répondants et les répondants qualifiés peuvent se retirer de cette étape d'approvisionnement à tout moment.

(h) Cette exigence est soumise aux dispositions de : l'Accord économique et commercial global entre le Canada et l'Union européenne (AÉCG), l'Accord marchés publics (AMP) de l'Organisation mondiale du commerce (OMC), l'Accord de libre-échange nord-américain (ALENA), l'Accord de libre-échange entre le Canada et le Chili (ALÉCC), l'Accord de libre-échange Canada–Pérou (ALÉCP), l'Accord de libre-échange Canada–Colombie (ALÉCCO), l'Accord de libre-échange Canada-Honduras (ALÉCH), l'Accord de libre-échange Canada-Corée (ALÉCRC), l'Accord de libre-échange Canada-Panama (ALÉCPA), l' Accord de partenariat transpacifique global et progressiste (PTPGP) et l'Accord de libre-échange canadien.

1.3 Renseignements sur le projet

Le projet a pour objectif général la sélection d'un entrepreneur unique aux fins de la mise au point d'un système de gestion de l'information relative au Programme d'aide aux employés (SGIPAE), en vue de répondre aux besoins de Santé Canada qui sont énoncés à l'annexe B, Ébauche d'énoncé des exigences (EDE), et seront définis plus en détail dans la DDS subséquente.

L'entrepreneur sélectionné dans le cadre du processus de la DDS se verra octroyer le contrat de mise au point du SGIPAE, dont la durée pourrait atteindre dix ans. Les exigences précises que devra respecter le SGIPAE et les conditions générales du contrat seront communiquées aux entrepreneurs ayant répondu à l'IQ que l'on aura autorisés à participer à l'étape de l'examen et de l'amélioration des exigences (EAE), puis au processus de la DDS subséquent, de la manière énoncée dans la partie 4, Procédure d'évaluation et sélection des répondants qualifiés, de la présente IQ.

La durée du contrat ne sera définie qu'à l'étape de la DDS, mais le Canada à l'intention d'utiliser le SGIPAE aussi longtemps que cela aura du sens de le faire du point de vue des opérations. La durée du contrat ne correspondra pas nécessairement à la durée de vie utile prévue pour la solution. Le contrat comprendra des options de prolongation pouvant être exercées dans le temps, au besoin. Le Canada souhaite aussi tirer avantage de toute évolution technologique (évolution du produit) qui pourrait advenir pendant la durée de vie utile du SGIPAE. Par conséquent, le contrat pourrait être modifié selon les besoins, afin que le Canada ait toujours accès au potentiel fondamental du produit, quelle que soit son évolution. Il est envisagé d'inclure parmi les éléments livrables du SGIPAE des services professionnels, une garantie, des services de maintenance et de soutien technique, de la formation et des ressources documentaires.

Le processus d'acquisition permettra aussi au Canada de rendre le SGIPAE accessible à tout ministère, à toute société d'État (aux termes de la *Loi sur la gestion des finances publiques*) et à toute autre partie pour le compte desquels le ministère des Travaux publics et des Services gouvernementaux est

autorisé à agir à l'occasion en vertu de l'article 16 de la *Loi sur le ministère des Travaux publics et des Services gouvernementaux* (chacun d'eux étant un « client »). Bien que le Canada puisse rendre le SGIPAE accessible à l'un ou l'autre ou à l'ensemble de ses clients, le présent processus d'acquisition n'empêche pas le Canada d'utiliser une autre méthode d'approvisionnement pour les entités du gouvernement du Canada ayant les mêmes besoins ou des besoins semblables.

1.3.1 Contexte du projet

Le groupe des Service d'aide aux employés (SAE) de Santé Canada gère le Programme d'aide aux employés (PAE) et de services connexes aux organismes publics fédéraux, aux ministères et aux organisations régies par le gouvernement fédéral.

Au sein de la Direction générale des services de gestion (DGSG) de Santé Canada, le SAE fait partie de la Direction des services de santé spécialisés (DSSS). Il offre en tout temps un accueil et un aiguillage entièrement bilingues en vue de services de conseil professionnels et confidentiels en personne, également bilingues. Le SAE fonctionne selon une formule de recouvrement complet des coûts et jouit du plein agrément du Council on Accreditation (COA). Le SAE compte près de 1 000 conseillers œuvrant en pratique privée aux quatre coins du pays et peut offrir son soutien à environ 1,6 million de clients admissibles (les employés et les membres de leur famille), répartis dans plus de 80 ministères et organismes fédéraux, dans les Forces armées canadiennes et dans la Gendarmerie royale du Canada, ainsi que parmi les vétérans. Le SAE est le plus vaste fournisseur de services de ce type auprès de la fonction publique fédérale.

Le PAE est le principal service que fournit le SAE. En 2019, le PAE a répondu à plus de 77 000 appels; au cours de l'exercice 2018-2019, il a géré près de 29 200 cas. On s'attend à ce que la demande de services auprès du PAE continue d'augmenter dans un proche avenir, en raison des efforts soutenus visant à réduire la stigmatisation de la maladie mentale et grâce à la récente initiative des milieux de travail sains prise par l'ancien greffier du Conseil privé, Michael Wernick.

À la suite d'une demande de renseignements (DDR) qu'a effectuée le Canada en 2018, on sait qu'il existe sur le marché des solutions toutes prêtes qui satisferaient aux principales exigences du PAE. La première catégorie de gens touchée par la mise en œuvre de la nouvelle solution serait celle des personnes qui participent à la prestation et à la gestion du PAE, comme les conseillers responsables des premiers contacts, les équipes de gestion des cas et le gestionnaire du centre d'appels. Les catégories touchées de façon secondaire par le changement seraient celle des fournisseurs de services et l'équipe du Bureau d'affaires, en raison de la mise à jour des processus.

1.3.2 Objectifs du projet

Les objectifs du projet sont les suivants :

1. garantir et mettre en œuvre une solution accessible en tout temps (disponibilité du système), dont le délai de réaction est rapide (performance du système) et dont l'utilisation est simple et facile à apprendre (convivialité);
2. disposer de données de qualité élevée provenant de diverses sources, accessibles aux utilisateurs sans trop d'efforts (qualité des données);
3. disposer d'une solution facilement transformable, c'est-à-dire qui permet l'ajout de champs ou de valeurs à des menus déroulants, le retrait de tels champs ou valeurs et la modification de tels champs ou valeurs, etc. afin de tenir compte de changements dans l'environnement de travail (souplesse du système);
4. mettre en œuvre une solution pouvant facilement être augmentée ou réduite (caractère modulable);
5. mettre en œuvre une solution efficace sur le plan des opérations;
6. assurer aux clients la confidentialité.

1.3.3 Environnement cible

L'environnement cible envisagé à cette étape préliminaire pour le SGIPEA est énoncé à l'annexe B, Ébauche d'énoncé des exigences. L'entrepreneur qui aura été sélectionné au moyen de l'IQ et du processus de DDS devra fournir et livrer un SGIPAE intégré, ayant les caractéristiques suivantes :

1. Le SGIPAE doit offrir l'éventail de fonctionnalités opérationnelles énoncées à la section 3.2 de l'annexe B, Ébauche d'énoncé des exigences, qui auront été clarifiées au cours du processus d'acquisition.
2. Le SGIPAE doit être déployé au sein de services d'infrastructure fournis par le gouvernement du Canada, comme cela est énoncé à l'appendice A de l'annexe B, Ébauche d'énoncé des exigences, et selon les clarifications qui auront été fournies au cours du processus d'acquisition.
3. Les services doivent comprendre la conception détaillée, la configuration, l'intégration et le déploiement du SGIPAE, la transition vers celui-ci, le soutien technique continu et l'éventuelle transition vers une solution ou des services ultérieurs, selon ce que prévoit la section 3.3 de l'annexe B, Ébauche d'énoncé des exigences, et selon les clarifications du processus d'acquisition.
4. Le SGIPAE doit être conforme aux exigences de sécurité du Canada, tel qu'elles sont énoncées dans l'IQ et auront été énoncées dans la DDS subséquente.

1.4 Aperçu du processus d'approvisionnement

Cette IQ est la première phase du processus d'approvisionnement pour le projet. Bien que le processus d'approvisionnement reste sujet à changement (et même à annulation, conformément aux Instructions uniformisées), le Canada prévoit actuellement que le processus d'approvisionnement se déroulera selon les phases suivantes :

1.4.1 Phase 1: Invitation à se qualifier (IQ)

L'objectif de cette IQ est de qualifier les répondants qui répondent aux exigences de l'IQ (Répondants Qualifiés). Un maximum de huit (8) répondants qualifiés les mieux classés seront invités à participer aux phases ultérieures du processus d'approvisionnement. Les répondants seront qualifiés et classés sur la base du processus défini dans la partie 4 de la présente IQ. En cas d'égalité entre deux ou plusieurs répondants comme 8^{e} et dernier répondant qualifié, le Canada sélectionnera tous les répondants qui se trouvent dans cette situation comme répondants qualifiés. S'il y a moins de huit (8) répondants qualifiés, tous les répondants qualifiés seront invités à participer aux étapes subséquentes. L'IQ sera affichée sur le Service électronique d'appels d'offres du gouvernement (SEAOG) pendant une période de vingt-cinq (25) jours civils, en anglais et en français.

Si le nombre de répondants qualifiés après la phase 1 est insuffisant pour permettre les phases ultérieures, le Canada se réserve le droit d'annuler toute phase ultérieure ou de modifier les exigences de la phase 1 et de publier à nouveau la demande de soumissions en utilisant la même approche ou une approche différente.

1.4.2 Phase 2 : Examen et amélioration des exigences (EAE)

Le processus d'examen et amélioration des exigences (EAE) avec les répondants qualifiés peut avoir lieu après la phase de l'IQ. L'objectif de la phase d'EAE est d'obtenir les commentaires des répondants qualifiés sur les exigences du Canada pour le projet, y compris l'ébauche de la DDS et les conditions du contrat qui en découle.

L'EAE est conçue comme un processus de collaboration et peut comporter des interactions telles que des ateliers, des séances individuelles et/ou des questions et réponses écrites. Le Canada tiendra compte des commentaires fournis par les répondants qualifiés lorsqu'il peaufinera les exigences et préparera ses documents d'approvisionnement pour le projet. De plus amples détails concernant l'EAE seront fournis aux répondants qui se qualifient grâce à cette IQ.

1.4.3 Phase 3 : Demande de soumissions (DDS)

Les informations fournies dans cette section ne représentent pas un engagement de la part du Canada et sont fournies uniquement à titre d'information. Elles peuvent être modifiées par le Canada à sa seule discrétion, au stade de la demande de soumissions.

Dans le cadre de la DDS, le Canada a l'intention d'inviter les répondants qualifiés à soumettre des propositions qui doivent contenir, en ce qui concerne le projet, une soumission technique et une soumission financière. La forme de la soumission sera décrite dans la DDS et portera à la fois sur les aspects techniques et financiers du projet et pourra inclure, à la discrétion du Canada, un contrôle de validité de la soumission. La demande de soumissions sera affichée sur le Service électronique d'appels d'offres du gouvernement (SEAOG) pendant une période de quarante (40) jours civils, en anglais et en français.

Le soumissionnaire retenu sera identifié en tenant compte des critères techniques et financiers énoncés dans la demande de soumissions. Les détails concernant les exigences de soumission pour la DDS et les facteurs à prendre en compte dans l'évaluation des soumissions seront indiqués dans la DDS.

1.5 Conflit d'intérêts - Avantage indu

Afin de protéger l'intégrité du processus d'approvisionnement, les répondants sont avisés que le Canada peut rejeter une soumission dans les circonstances suivantes :

a) Si le répondant, un de ses sous-traitants, un de leurs employés respectifs, actuels ou anciens, a participé d'une manière ou d'une autre à la préparation de stratégies ou de documents reliés au processus d'approvisionnement ou est en situation de conflit d'intérêts ou d'apparence de conflit d'intérêts;

b) Si le répondant, un de ses sous-traitants, un de leurs employés respectifs, actuels ou anciens, a eu accès à des renseignements liés au processus d'approvisionnement qui n'étaient pas disponibles aux autres fournisseurs et que le cas échéant aurait, selon le Canada, donné ou aurait l'apparence d'avoir donné au répondant un avantage indu.

À cet égard, le Canada informe qu'il a utilisé les services des consultants/entrepreneurs du secteur privé suivants afin de préparer les stratégies ou documents reliés au processus d'approvisionnement :

Prénom	Nom de famille	Organisation
Jocelyn	Décoste	BDO Canada LLP
John	Davis	BDO Canada LLP

Le Canada ne considère pas, qu'en soi, l'expérience acquise par un répondant qui fournit ou a fourni les biens et services décrits dans la demande de soumissions (ou des biens et services semblables) représente un avantage indu en faveur du répondant ou crée un conflit d'intérêts. Ce répondant demeure cependant assujetti aux critères énoncés plus hauts.

Dans le cas où le Canada a l'intention de rejeter une réponse conformément au présent article, l'autorité contractante préviendra le répondant et lui donnera la possibilité de faire valoir son point de vue, avant de prendre une décision définitive. Les répondants ayant un doute par rapport à une situation particulière devraient contacter l'autorité contractante avant la date de clôture de la demande de soumissions. En présentant une réponse, le répondant déclare qu'il n'est pas en conflit d'intérêts et qu'il ne bénéficie d'aucun avantage indu. Le répondant reconnaît que le Canada est seul habilité à établir s'il existe un conflit d'intérêts, un avantage indu ou une apparence de conflit d'intérêts ou d'avantage indu.

1.6 **Compte rendu**

Les répondants peuvent demander une séance pour recevoir un compte rendu au sujet de leurs résultats obtenus à la suite de l'étape d'IQ. Les répondants doivent faire parvenir leur demande au plus tard 5 jours ouvrables à partir de la réception de leurs résultats obtenus suite au processus de qualification décrit dans ce document.

PARTIE 2 : INSTRUCTIONS POUR LA PRÉSATION DES RÉPONSES

2.1 Instructions, clauses et conditions uniformisées

(a) Toutes les instructions, clauses et conditions identifiées dans l'IQ par un numéro, une date et un titre sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices /guide-des-clauses-et-conditionsuniformisees-d-achat) publié par Travaux publics et Services gouvernementaux Canada.

(b) Les répondants qui présentent une réponse s'engagent à respecter les instructions, les clauses et les conditions de l'IQ.

(c) Le document 2003 (2019-03-04), Instructions uniformisées – biens ou services – besoins concurrentiels, est incorporé par renvoi dans l'IQ et en fait partie intégrante, sauf :

(i) lorsque l'expression " demande de soumissions " est utilisée, la remplacer par " Invitation à se qualifier (IQ) " ;

(ii) lorsque le terme " soumission " est utilisé, le remplacer par " réponse " ;

(iii) lorsque le terme " soumissionnaire " est utilisé, le remplacer par " répondant ".

(iv) Le paragraphe 5 (4), qui traite d'une période de validité, ne s'applique pas, étant donné que l'IQ invite simplement les répondants à se qualifier. À moins que le répondant n'informe l'autorité contractante par écrit de son désir de retirer sa réponse, le Canada présumera que tous les répondants qui soumettent une réponse continuent de vouloir se qualifier.

(d) En cas de divergence entre les clauses du document 2003 et de la présente, les dispositions pertinentes de la présente prévalent.

2.2 Présentation de la réponse

(a) Les réponses doivent être présentées uniquement à l'Unité de réception des soumissions de Travaux publics et Services gouvernementaux Canada, au plus tard à la date, à l'heure et à l'endroit indiqués dans l'IQ.

(b) Si le répondant choisit de soumettre sa réponse par voie électronique, le Canada demande que le répondant soumette sa réponse conformément à la section 08 des instructions uniformisées de 2003. Le système Connexion postel a une limite de 1 Go par message publié et une limite de 20 Go par conversation.

Les formats approuvés pour les documents sont n'importe quelle combinaison de:

A. Documents PDF; et
B. Documents pouvant être ouverts avec Microsoft Word ou Microsoft Excel.

La réponse doit être organisée par sections et séparée comme suit:

A. Section I: Critères de sélection obligatoires et cotés de l'IQ (tels que décrits à l'annexe C - Critères d'évaluation et de qualification)

B. Section II: Attestations et informations supplémentaires

(c) Si le répondant choisit de soumettre sa réponse sur support électronique, le Canada demande que le répondant présente sa réponse dans des sections organisées séparément comme suit:

A. Section I: Critères de qualification obligatoires et cotés de l'IQ (tels que décrits à l'annexe C - Critères d'évaluation et de qualification) (2 copies électroniques sur clés USB)

B. Section II: Attestations et informations supplémentaires (2 copies électroniques sur clés USB)

(d) Si le répondant fournit simultanément des copies de sa réponse en utilisant plusieurs méthodes de livraison acceptables, et s'il y a une différence entre le libellé de l'une de ces copies et la copie électronique fournie par le biais du service Connexion postel, le libellé de la copie électronique fournie via le service Connexion postel aura la priorité sur le libellé des autres copies.

(e) Veuillez noter qu'aucun prix ne doit être indiqué dans la réponse à l'IQ.

(f) En raison de la nature de cette IQ, les réponses transmises par télécopieur ne seront pas acceptées.

2.3 Demandes de renseignements

(a) Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins 5 jours civils avant la date de clôture de l'IQ. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible que le Canada ne puisse pas y répondre.

(b) Les répondants doivent acheminer les demandes de renseignements au sujet de l'IQ à :

Autorité contractante : Ngoma Nkiama

Courriel : ngoma.nkiama@tpsgc-pwgsc.gc.ca

(c) Les répondants devraient indiquer le plus fidèlement possible le numéro de l'article de l'IQ auquel se rapporte leur demande de renseignements et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude.

(d) Les demandes de renseignements qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention «exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au répondant de le faire, afin d'en éliminer le caractère exclusif et de permettre la transmission des réponses à tous les répondants. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permettrait pas de les diffuser à tous les parties intéressées.

2.4 Expérience de co-entreprise

(i) Sauf indication contraire, si le répondant est une coentreprise qui possède de l'expérience à ce titre, il peut citer l'expérience qu'il a acquise en tant que coentreprise. Un répondant d'une coentreprise qui présente une soumission peut évoquer l'expérience de l'un de ses membres pour démontrer qu'il satisfait à toute exigence obligatoire de la présente IQ.

(ii) Des membres de la coentreprise ne peuvent cependant pas mettre leurs capacités en commun avec celles d'autres membres pour démontrer qu'ils satisfont à une exigence obligatoire de la présente IQ. Toutefois, un membre de la coentreprise peut ajouter à son

expérience individuelle celle de la coentreprise elle-même. Lorsqu'il est nécessaire de justifier une expérience, le répondant doit préciser le membre de la coentreprise qui satisfait à l'exigence.

(iii) Les répondants qui ont des questions concernant l'évaluation des soumissions présentées par des coentreprises devraient les poser dans le cadre du processus de demande de renseignements, le plus tôt possible durant la période de l'IQ.

(iv) Exemple 1 : Un répondant est membre d'une coentreprise composée de X, Y et Z. Si, dans la réponse, on exige que : a) le répondant ait trois ans d'expérience dans la prestation de services de maintenance, et b) que le répondant ait deux ans d'expérience dans l'intégration de matériel dans des réseaux complexes, chacune de ces deux exigences peut être satisfaite par un membre différent de la coentreprise. Cependant, pour une exigence donnée, par exemple celle qui concerne l'expérience de trois (3) ans de la prestation de services d'entretien, le répondant ne peut pas indiquer que chaque membre, soit X, Y et Z, a un an d'expérience pour un total de trois (3) ans. Une telle réponse serait déclarée non conforme.

(v) Exemple 2 : Supposons que le répondant est une coentreprise constituée des membres L et M, et que la réponse exige que le répondant démontre de l'expérience dans la prestation de services de maintenance et de dépannage à un client comptant au moins 10 000 utilisateurs, pendant 24 mois. Le répondant (en tant que coentreprise formée des membres L et M) a déjà fourni ces services par le passé. Il peut donc utiliser cette expérience pour satisfaire à l'exigence (même si ni L, ni M ne satisfont individuellement à l'exigence relative à l'expérience). Toutefois, si le membre L a acquis cette expérience alors qu'il formait une coentreprise avec une autre entreprise (le membre N), le répondant ne peut pas indiquer cette expérience parce que le membre N ne fait pas partie de la coentreprise qui présente une soumission dans le cadre de l'IQ.

(vi) Exemple 3 : Un répondant est membre d'une coentreprise composée de A et B. Si, dans une réponse, on exige que le soumissionnaire ait de l'expérience dans la prestation de ressources pour un minimum de 100 jours facturables, le répondant peut démontrer son expérience en présentant ce qui suit :

- les contrats signés par A, ou
- les contrats signés par B, ou
- les contrats signés par A et B en coentreprise, ou
- les contrats signés par A et les contrats signés par B en coentreprise, ou
- les contrats signés par B et les contrats signés par A et B en coentreprise,

pour un total de 100 jours facturables.

2.5 Lois applicables

Les relations entre les parties seront régies par les lois en vigueur dans la province de l'Ontario, Canada.

Avis à l'intention des répondants : À leur discrétion, les répondants peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur réponse ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que le répondant accepte les lois applicables indiquées. Les répondants devraient indiquer dans leur formulaire principal de soumission de l'IQ la province ou le territoire Canadien qu'ils souhaitent que leurs réponses soient appliquées.

PARTIE 3 : INSTRUCTIONS POUR LA PRÉSENTATION DE LA RÉPONSE

3.1 Instructions pour la présentation des réponses

(a) Le Canada demande aux répondants de fournir leur réponse en sections distinctes, réparties comme suit :

(i) Section I : Réponse de qualification aux exigences obligatoires de l'IQ (telles décrites à l'annexe C)

(ii) Section II : Attestation(s)

L'information sur l'établissement des prix n'est pas une exigence et ne devrait pas être incluse dans la réponse.

(b) **Langue pour les communications futures** : Les répondants devraient indiquer dans le Formulaire de présentation de la réponse à l'IQ la langue officielle du Canada préférée (anglais canadien ou français canadien) pour être utilisée à l'avenir dans les communications entre le Canada et le répondant, concernant ce processus d'approvisionnement.

3.2 Réponse de qualification

Dans leur réponse, les répondants doivent démontrer comment ils ont les compétences requises d'une manière complète, claire et concise. Il n'est pas suffisant de simplement répéter les critères.

(a) Une réponse de qualification comprend ce qui suit :

(i) **Formulaire principal de soumission de l'IQ:** Il est demandé aux répondants de joindre le formulaire principal de soumission de l'IQ avec leurs réponses. Il s'agit d'un formulaire commun dans lequel les répondants peuvent fournir les renseignements requis pour fins d'évaluation, comme le nom d'une personne-ressource, le numéro d'entreprise - approvisionnement du répondant, le statut du répondant au Programme de contrats fédéraux (PCF) pour l'équité en matière d'emploi etc. L'utilisation de ce formulaire pour fournir les renseignements n'est pas obligatoire, mais recommandée. Si le Canada considère que les renseignements requis par le formulaire de présentation des réponses sont incomplets ou doivent être corrigés, le Canada accordera au répondant la chance de compléter ou de corriger ces renseignements.

(ii) **Critères obligatoires pour se qualifier** : La réponse technique doit prouver la conformité aux critères précis des exigences obligatoires relatives à la sélection, comme il est énoncé à l'annexe C. La justification ne doit pas être une simple répétition du besoin, mais doit expliquer et démontrer la façon dont le répondant satisfera aux exigences et exécutera les travaux exigés. Il n'est pas suffisant de simplement déclarer que le répondant, la solution ou les ressources qu'il propose, est conforme. Lorsque le Canada détermine que la justification n'est pas complète, le répondant sera jugé non conforme et sa soumission sera rejetée. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse.

(iii) **Critères de qualification cotés** : La réponse technique devrait justifier la conformité avec les critères spécifiques des Exigences de Qualification Cotés comme disposé à l'Annexe C. Les critères dans cette section, bien que non obligatoire en soient, ils seront utilisés pour établir un classement des répondants qui rencontrent les Critères de qualification obligatoires décrites dans la section (ii) ci-dessus. La justification ne doit pas être simplement une répétition de l'exigence, mais doit expliquer et démontrer comment le répondant satisfait les besoins. Déclarer simplement que le répondant ou sa solution proposée ou les ressources se conforment n'est pas suffisant. Où le Canada résout que la justification n'est pas complète, le répondant ne recevra pas un score pour ce critère donné. La justification peut faire allusion à la documentation supplémentaire soumise avec la réponse.

(iv) **Formulaires de Références des Projets précédents** : les répondants sont demandés d'utiliser le Formulaire C-1 – Reference de déploiements antérieurs des solutions de logiciel, où la conformité est déterminée par le biais d'une mise en œuvre de solution de référence de client externe. Bien que tout le contenu du formulaire C-1 soit exigé, utiliser le formulaire lui-même pour fournir ces renseignements n'est pas obligatoire. Pour les répondants qui utilisent un formulaire différant, c'est dans la discrétion unique du Canada pour déterminer si tous les renseignements exigés ont été fournis. Les modifications aux déclarations dans le Formulaire C-1 peuvent avoir pour résultat que la réponse soit déclarée non-conforme. Le répondant devrait, au minimum, fournir la réponse pour le nom, le titre, le numéro de téléphone, le courriel et le rôle de la personne contact du client externe qui avait le mandat de supervision ou l'autorité d'approbation des travaux. Si les renseignements de la personne contact du client externe ne sont pas fournis avec la réponse, l'Autorité contractante informera le répondant et lui donnera un délai pour soumettre les renseignements. Le défaut de se conformer à la demande de l'Autorité contractante et satisfaire les besoins dans la période de temps rendra la réponse non-conforme. Si l'individu désigné est non disponible pendant la période d'évaluation, le répondant peut fournir le nom et les renseignements d'un autre contact du même client externe. Si les références du client externe sont fournies plus que demandées, le Canada évaluera les références dans l'ordre qu'ils ont été soumis par le répondant jusqu'au nombre de références demandées.

PARTIE 4 : PROCEDURES D'ÉVALUATION ET SÉLECTION DES RÉPONDANTS QUALIFIÉS

4.1 Procédures d'évaluation

(a) Les réponses seront évaluées par rapport à l'ensemble des exigences de l'IQ, incluant les critères de qualification obligatoires et les critères de qualification cotés. La méthode d'évaluation comporte plusieurs étapes, qui sont décrites ci-après. Même si l'évaluation et la sélection seront effectuées par étape, le fait que le Canada soit passé à une étape ultérieure ne signifie pas que ce dernier a irréfutablement déterminé que le répondant a réussi toutes les étapes précédentes. Le Canada se réserve le droit d'exécuter parallèlement certaines étapes de l'évaluation.

(b) Une équipe constituée de représentants du Canada évaluera les réponses. Le Canada peut faire appel à des experts-conseils ou à toute personne-ressource du gouvernement pour évaluer les réponses. Tous les membres de l'équipe d'évaluation ne participeront pas nécessairement à tous les aspects de l'évaluation.

(c) En plus de tous les autres délais prescrits dans l'IQ :

(i) **Demandes de précisions :** si le Canada demande des précisions au répondant sur sa réponse ou qu'il veut vérifier la réponse, le répondant disposera d'un délai de deux jours ouvrables (ou d'un délai plus long précisé par écrit par l'autorité contractante) pour fournir les renseignements nécessaires au Canada. À défaut de respecter ce délai, sa réponse sera jugée non recevable.

(ii) **Demandes de renseignements supplémentaires** : si le Canada demande des renseignements supplémentaires conformément à la section «Déroulement de l'évaluation» du document 2003, Instructions uniformisées – biens ou services – besoins concurrentiels, afin de :

(A) vérifier tout renseignement fourni par le répondant dans sa réponse ;

(B) communiquer avec une ou toutes les références citées par le répondant dans le but de valider les renseignements fournis par le répondant,

le répondant doit soumettre les renseignements demandés par le Canada dans les 2 jours ouvrables suivant la demande de l'autorité contractante.

(iii) **Prolongation du délai** : si le répondant a besoin de davantage de temps, l'autorité contractante, à sa seule discrétion, peut accorder une prolongation du délai.

4.2 Evaluation des réponses

(a) **Exigences obligatoires pour se qualifier:** Chaque réponse sera examinée pour déterminer si elle satisfait aux exigences obligatoires de l'IQ. Tous les éléments de l'IQ qui constituent des exigences obligatoires sont désignés par les termes " doit ", " doivent " ou " obligatoire ". Les réponses qui ne sont pas conformes à chacune des exigences obligatoires seront jugées non recevables et seront rejetées.

(b) **Exigences de qualifications cotées :** Chaque réponse sera cotée en attribuant une note aux exigences cotées, qui sont identifiées dans l'IQ par le mot «coté» ou par référence à une note. Le répondant qui ne soumet pas de réponse complète avec toutes les informations demandées par cette IQ sera évalué en conséquence. Les critères de qualification cotés sont décrits à l'annexe C - Critères d'évaluation et de qualification.

4.3 Vérification de références

(a) Le Canada effectuera la vérification des références par écrit par courriel. Le Canada enverra toutes les demandes de vérification des références par courriel aux personnes-ressources fournies par tous les répondants le même jour en utilisant le courriel fournie dans la réponse. Un répondant ne satisfera pas à l'exigence d'expérience obligatoire (le

cas échéant) à moins que la réponse ne soit reçue dans les 10 jours ouvrables suivant la date d'envoi du courriel du Canada.

(b) Le cinquième jour ouvrable après l'envoi de la demande de vérification des références, si le Canada n'a pas reçu de réponse, le Canada avisera le répondant par courriel, afin de permettre au répondant de contacter sa référence directement pour s'assurer qu'il répond au Canada dans les 10 jours ouvrables. Si la personne nommée par un répondant n'est pas disponible lorsque requis pendant la période d'évaluation, le répondant peut fournir le nom et le courriel d'une autre personne-ressource du même client. Les répondants n'auront cette possibilité qu'une seule fois pour chaque client, et uniquement si la personne nommée à l'origine n'est pas disponible pour répondre (c.-à-d., le répondant n'aura pas la possibilité de soumettre le nom d'une autre personne-ressource si la personne-ressource d'origine indique qu'il ne veut pas ou ne peut pas répondre). Les 10 jours ouvrables ne seront pas prolongés pour donner plus de temps au nouveau contact pour répondre.

(c) Lorsque les informations fournies par une référence diffèrent des informations fournies par le répondant, les informations fournies par la référence seront les informations évaluées.

(d) Les points ne seront pas attribués et / ou un répondant ne satisfera pas à l'exigence d'expérience obligatoire (le cas échéant) si (1) le client de référence déclare qu'il n'est pas en mesure ou ne veut pas fournir les informations demandées, ou (2) le client de référence n'est pas un client du répondant lui-même (par exemple, le client ne peut pas être le client d'un affilié du répondant au lieu d'être un client du répondant lui-même). Les points ne seront pas non plus attribués ou obligatoires si le client est lui-même un affilié ou une autre entité qui a un lien de dépendance avec le répondant.

(e) La décision de procéder ou non à la vérification des références est discrétionnaire. Cependant, si le Canada choisit d'effectuer une vérification des références pour toute exigence cotée ou obligatoire, il vérifiera les références de cette exigence pour tous les répondants qui, à ce stade, n'ont pas été jugés non conformes.

4.4 Évaluation de la viabilité financière

Le répondant doit avoir la capacité financière nécessaire pour répondre à ce besoin. Afin d'évaluer la capacité financière du répondant, l'autorité contractante pourra, dans un avis écrit à l'intention du répondant, exiger que ce dernier fournisse une partie ou la totalité des renseignements financiers dont il est question ci-dessous durant l'évaluation des réponses.

Le répondant doit fournir à l'autorité contractante les renseignements suivants dans un délai de cinq (5) jours ouvrables suivant la réception d'une demande de l'autorité contractante ou dans un délai précisé par l'autorité contractante dans l'avis.

(a) Les états financiers vérifiés ou, si ces derniers ne sont pas disponibles, les états financiers non vérifiés (préparés par la firme de comptabilité externe du répondant, s'il y a lieu, ou encore préparés à l'interne si aucun état financier n'a été préparé par un tiers) pour les trois derniers exercices financiers du répondant ou, si l'entreprise est en opérations depuis moins de trois ans, pour toute la période en question (incluant au minimum le bilan, l'état des bénéfices non répartis, l'état des résultats et les notes afférentes aux états financiers).

(b) Si les états financiers mentionnés au paragraphe a) datent de plus de cinq mois précédant la date à laquelle l'autorité contractante demande l'information, le répondant doit également fournir, à moins que ce soit interdit par une loi dans le cas des sociétés ouvertes au public, les derniers états financiers trimestriels (comprenant un bilan et un état des résultats depuis le début de l'exercice), datant de deux mois précédant la date à laquelle l'autorité contractante demande cette information.

(c) Si le répondant n'exerce pas ses activités depuis au moins un exercice complet, il doit fournir les renseignements suivants :

i. le bilan d'ouverture en date de début des activités (dans le cas d'une corporation, un bilan à la date de la constitution de la société);

ii. les derniers états financiers trimestriels (comprenant un bilan et un état des résultats depuis le début de l'exercice) datant de deux mois précédant la date à laquelle l'autorité contractante demande cette information.

(d) Une attestation de la part du directeur financier ou d'un signataire autorisé du soumissionnaire stipulant que les renseignements financiers fournis sont exacts et complets.

Si le répondant est une coentreprise, les renseignements financiers exigés par l'autorité contractante doivent être fournis par chaque membre de la coentreprise.

Si le répondant est une filiale d'une autre entreprise, alors les renseignements financiers mentionnés aux paragraphes a) à d) exigés par l'autorité contractante doivent être fournis par la société mère elle-même.

Le répondant n'est pas tenu de soumettre de nouveau des renseignements financiers demandés par l'autorité contractante qui sont déjà détenus en dossier à TPSGC par la Direction des services des politiques, de la vérification et de l'analyse des coûts du Secteur de la politique, du risque, de l'intégrité et de la gestion stratégique, à condition que dans le délai susmentionné :

(a) le répondant indique par écrit à l'autorité contractante les renseignements précis qui sont en dossier et le besoin à l'égard duquel ces renseignements ont été fournis;

(b) le répondant autorise l'utilisation de ces renseignements pour ce besoin.

Il incombe au répondant de confirmer auprès de l'autorité contractante que ces renseignements sont encore détenus par TPSGC.

Le Canada se réserve le droit de demander au répondant de fournir tout autre renseignement requis par le Canada pour procéder à une évaluation complète de la capacité financière du répondant.

Confidentialité : Si le répondant fournit au Canada, à titre confidentiel, les renseignements exigés ci-dessus et l'informe de la confidentialité des renseignements divulgués, le Canada doit traiter ces renseignements de façon confidentielle, suivant les dispositions de la Loi sur l'accès à l'information, L.R., 1985, ch. A-1, alinéas 20(1)b) et c).

4.5 Sélection des répondants qualifiés

Une réponse doit être conforme aux exigences de l'IQ, satisfaire à toutes les exigences d'évaluation technique obligatoires et obtenir les notes minimales requises pour les exigences d'évaluation côtés, comme indiqué à l'annexe C - Critères d'évaluation et de qualification, pour être déclarée recevable.

Pour chaque réponse, la note obtenue pour chacune des exigences d'évaluation cotée sera additionnée pour obtenir une note globale totale.

Les huit (8) répondants qualifiés ayant obtenu la note globale totale la plus élevée seront sélectionnés comme répondants qualifiés pour participer à toute phase ultérieure du processus d'approvisionnement.

En cas d'égalité entre deux ou plusieurs répondants en tant que 8e et dernier répondant qualifié, le Canada sélectionnera tous les répondants qui se trouvent dans cette situation comme répondants qualifiés.

S'il y a moins de 8 répondants qualifiés, tous les répondants qualifiés seront sélectionnés pour participer aux phases ultérieures du processus d'approvisionnement. Si le nombre de répondants qualifiés est insuffisant après l'étape de l'IQ pour permettre une compétition dans les étapes subséquentes du processus d'approvisionnement, le Canada se réserve le droit d'annuler toute étape subséquente du processus d'approvisionnement afin de modifier les exigences de l'étape de l'IQ et de publier à nouveau la demande de soumissions en utilisant la même approche ou une approche différente.

Le Canada se réserve le droit de réévaluer la qualification de tous répondants qualifiés à tout moment au cours du processus d'approvisionnement.

4.6 Invitation à signer une entente de répondant

L'autorité contractante invitera un maximum de huit (8) répondants qui se sont qualifiés conformément à la section 4.5 ci-dessus à signer l'entente de répondant, comme condition pour être sélectionnés pour participer à toute phase ultérieure du processus d'approvisionnement.

Si l'un de ces répondant qualifiés échoue ou refuse d'exécuter l'entente de répondant dans le délai imparti, l'autorité contractante peut, à sa seule discrétion, retirer l'invitation et l'étendre au répondant qualifié suivant le mieux classé pour qu'il signe l'accord de soumission et participe à toutes les phases ultérieures du processus d'approvisionnement conformément à l'accord de soumission.

PARTIE 5: ATTESTATIONS

(a) Les répondants doivent fournir les attestations pour être déclarée un répondant retenu. Les attestations que les répondants remettent au Canada peuvent faire l'objet d'une vérification à tout moment par le Canada. Le Canada déclarera une réponse non recevable, ou à un manquement de la part de l'entrepreneur à l'une de ses obligations prévues au contrat, s'il est établi qu'une attestation du répondant est fausse, sciemment ou non, que ce soit pendant la période d'évaluation, ou pendant la durée du contrat. L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du répondant. À défaut de répondre et de coopérer à toute demande ou exigence imposée par l'autorité contractante, la réponse peut être déclarée non recevable, ou constituer un manquement aux termes du contrat.

(b) Les attestations et les renseignements supplémentaires énumérés ci-dessous devraient être remplis et fournis avec la réponse mais ils peuvent être fournis plus tard. Si l'une de ces attestations et les renseignements supplémentaires ne sont pas remplis et fournis tel que demandé, l'autorité contractante informera le répondant du délai à l'intérieur duquel les renseignements doivent être fournis. À défaut de fournir les attestations énumérées ci-dessous dans le délai prévu, la réponse sera déclarée non recevable.

5.1 Dispositions relatives à l'intégrité - Déclaration de condamnation à une infraction

(a) Conformément au paragraphe Déclaration de condamnation à une infraction de l'article 01 des instructions uniformisées, le répondant doit, selon le cas, présenter avec sa réponse le Formulaire de déclaration (http://www.tpsgc-pwgsc.gc.ca/ci-if/formulaire-form-fra.html) dûment rempli afin que sa réponse ne soit pas rejetée du processus d'approvisionnement.

ANNEXES ET FORMULAIRES

ANNEXE A – DEFINITIONS ET INTERPRETATION

1. Sigles

Sigle	Définition
AE	Autorisation d'exploitation
AQ	Assurance de la qualité
ASI	Attestation de sécurité d'installation
AT	Autorisation de tâche
DP	Demande de propositions
EB	Énoncé des besoins
GC	Gouvernement du Canada
GDC	Gestion des cas
LVERS	Liste de vérification des exigences relatives à la sécurité
ODR	Objectifs de délai de rétablissement
PB	Protégé B
RAS	Reprise après sinister
RTPC	Réseau téléphonique public commuté
SGIPAE	Système de gestion de l'information relative au Programme d'aide aux employés
SPAC	Services publics et Approvisionnement Canada
SPC	Services partagés Canada
TPSGC	Travaux publics et Services gouvernementaux Canada, aussi connu sous le nouveau nom de Services publics et Approvisionnement Canada (SPAC)
VOD	Vérification d'organisation designée

2. **Definitions**

Termes	Signification
Application	Tout programme ou groupe de programmes conçu pour l'utilisateur final, y compris les documents connexes, le code source, les supports, les données et les bases de données nécessaires à des tâches particulières de traitement des données et de télécommunication.
Attestation de sécurité d'installation (ASI)	Cote de sécurité qui autorise la personne qui la possède et ses employés ayant l'habilitation de sécurité requise à accéder à des renseignements sensibles ou à des lieux de travail à accès restreint.
Autorisation d'exploitation	Une autorisation d'exploitation (AE) est une déclaration officielle d'une autorité approbatrice désignée (AAD) qui autorise l'exploitation d'une solution informatique et approuve expressément le risque que celle-ci représente pour les activités de l'organisme. L'AE est signée après certification par un agent de certification (AC) selon laquelle le système respecte ou dépasse toutes les exigences de sécurité nécessaires à son exploitation. Une autorisation provisoire d'exploitation peut être délivrée pour une courte période ou à certaines conditions en attendant la décision d'approbation ou de rejet de la demande. Dans le contexte du contrat relatif à la présente, l'agent de certification responsable de l'ultime décision sera la Sécurité des TI d'EDSC.
Autorisation de tâches (AT)	L'AT est un outil administratif structuré qui permet à TPSGC ou à un client d'autoriser le travail d'un entrepreneur lorsque la situation l'exige, conformément aux conditions du contrat.
Autorité adjudicatrice	Autorité définie dans le sommaire des renseignements clés.

Termes	Signification
Calendrier principal du projet	Le calendrier principal du projet indique les principales étapes en matière de résultats opérationnels, d'éléments livrables et de dates cibles associées au passage du SGIPAE actuel au SGIPAE que fournira l'entrepreneur sélectionné.
Canada	Sa Majesté la Reine du chef du Canada, représentée par la ministre des Travaux publics et des Services gouvernementaux du Canada
Centre de données	Installations de l'entrepreneur ou d'un tiers qui accueillent des serveurs informatiques en réseau, généralement employées par les organisations pour le traitement centralisé des appels, les services de gestion de réseau ou le stockage, le traitement ou la distribution à distance de grandes quantités de données.
Coentreprise	Une coentreprise est une association de deux parties ou plus, qui rassemblent leurs fonds, leurs biens, leurs connaissances, leur expertise et d'autres ressources en une seule entreprise conjointe, parfois appelée « consortium », en vue d'opérations communes. Dans un contrat, les parties seront définies comme conjointes et solidaires.
Critères de qualification cotés	Critères de qualification cotés énoncés à l'annexe C, Critères d'évaluation et de qualification.
Demande de renseignements	Au sens de la partie 2.3 de la présente IQ
Demande de services	Demande de services envoyée à l'entrepreneur en vue de travaux qui s'inscrivent dans le cadre de l'AE.
Documentation	Documents, sur support papier ou électronique, y compris des guides d'installation, des instructions, des plans, des documents de maintenance, des manuels, des documents au sujet du système, des documents de formation et des guides d'utilisation, ainsi que les ajouts aux éléments qui précèdent et les modifications apportées à ceux-ci.
DP	La demande de propositions, selon ses différentes versions au fil du temps.
Employé	Personne se trouvant dans une relation officielle employeur-employé avec le soumissionnaire ou l'entrepreneur, tel que la définit l'Agence du revenu du Canada (ARC).
Entrepreneur	Personne, entité ou entités dont le nom figure au contrat et qui fournissent au Canada des biens, des services ou les deux.
Entreprise autochtone	Aux fins de la présente invitation, une entreprise autochtone est : a. une bande, aux termes de la *Loi sur les Indiens*; b. une entreprise individuelle; *OU* c. une société par actions à responsabilité limitée; d. une coopérative; e. une société de personnes; f. un organisme sans but lucratif au sein duquel des Autochtones disposent d'au moins 51 pour cent de la participation et du contrôle; OU g. une coentreprise consistant en deux entreprises autochtones ou plus ou en une ou plusieurs entreprises autochtones et en une ou plusieurs entreprises non autochtones, dans la mesure où la ou les entreprises autochtones disposent d'au moins 51 pour cent de la participation et du contrôle de la coentreprise; si une entreprise autochtone compte six employés à temps plein ou plus au moment de présenter sa soumission, au

Termes	Signification
	moins 33 pour cent d'entre eux doivent être des Autochtones, et cette proportion doit être maintenue tout au long du contrat.
Équipe de répondants	Répondant et tous les membres de son équipe.
Équipe principale du projet	Les fonctions et les personnes qui occupent les fonctions constituant l'essentiel des ressources de l'équipe du projet de mise en œuvre fournies par l'entrepreneur pour la réalisation du travail. L'équipe principale du projet doit compter les fonctions suivantes : 1. Cadre responsable 2. Gestionnaire du projet/compte 3. Responsable de la configuration et du déploiement de la solution logicielle de SGIPAE 4. Responsable de la configuration et du déploiement de l'infrastructure technique du SGIPAE 5. Responsable des services d'intégration de la solution de SGIPAE 6. Responsable des services et du soutien permanents de la solution de SGIPAE
Essai d'acceptation	Tout essai de l'ensemble ou d'un des éléments livrables qu'effectueront le Canada ou ses représentants pour déterminer si les éléments livrables sont conformes aux exigences, aux spécifications, aux garanties et aux normes énoncées ou intégrées dans l'énoncé des besoins.
Essai d'acceptation par l'utilisateur	Étape des essais au cours de laquelle le ou les utilisateurs de l'organisation cliente font l'essai de l'application pour s'assurer qu'elle fonctionne, qu'elle satisfait les besoins opérationnels et qu'elle est conforme aux exigences exprimées dans l'énoncé des besoins au sujet de l'application.
Gestion des incidents	Selon l'ITIL, version 3.0, la « gestion des incidents d'entreprise » (GIE) est le processus qui consiste à s'occuper des incidents.
Heures d'ouverture	Heures allant de 6 h à 18 h au cours d'un jour ouvrable à l'emplacement où le travail est effectué.
Incident	Au sens de la définition de l'ITIL, version 3.0, interruption non planifiée d'un service informatique ou réduction de la qualité d'un service informatique.
Installation(s)	Emplacement(s) au sein du territoire souverain du Canada à partir duquel ou desquels l'entrepreneur fournira au Canada les services relatifs au SGIPAE dont il a besoin ou assurera la prestation de tels services.
ITIL	*Information Technology Infrastructure Library*. Voir le site https://www.itlibrary.org/
Jour ouvrable	Un jour autre que le samedi, le dimanche ou un jour férié en Ontario.
Modification	Un ajout au document de demande de soumissions ou à un accord ou contrat subséquent, quel qu'il soit, la suppression d'un élément de ces documents, la correction d'un tel élément ou encore sa modification.
Modulabilité	Possibilité d'exploiter une solution logicielle sur un système de la taille qui convient et de la déplacer dans un système plus petit ou plus grand au besoin.
Objectif de délai de rétablissement (ODR)	Délai maximal et niveau de service d'un processus opérationnel exigés pour reprise après sinistre d'un processus.
Objectif de point de rétablissement (OPR)	Période maximale tolérée durant laquelle des données peuvent être perdues par un service des TI à cause d'un incident grave.
Offerts sur le marché (Disponibilité commerciale)	« Offerts sur le marché » signifie que les logiciels ou services proposés sont librement offerts à l'achat, qu'ils ont une définition de produit ou de service publiée et une structure de prix et disposent en permanence d'investissements de développement et de soutien. Dans le cas où la solution consiste en de multiples produits indépendants, chaque produit proposé doit être « offert sur le marché », selon la définition ci-dessus. Les versions ALPHA et BÊTA d'un produit ou d'un

Termes	Signification
	service NE remplissent PAS les conditions qui permettraient de les désigner comme « offertes sur le marché ».
Plateforme	Ensemble des composants des systèmes d'information de portée générale qui servent au traitement et au stockage de données électroniques, tels que les ordinateurs, les serveurs, les dispositifs de réseau et les appareils mobiles. Une plateforme comprend habituellement du matériel serveur, du matériel de stockage, du matériel destiné aux utilitaires, des logiciels et des systèmes d'exploitation.
Produit	Tout élément dont les droits sont réservés ou dont la marque a été déposée ayant été fabriqué ou étant offert à la vente dans le commerce et étant aisément identifiable au nom de son fabricant, de son modèle ou de son numéro de version.
Projet	Comme l'indiquent la section 1.3 et, de manière plus détaillée, l'annexe B, Énoncé des besoins, la fourniture d'un SGIPAE et de services connexes en appui au Programme d'aide aux employés du gouvernement du Canada, chez Santé Canada.
Proposition	Proposition officielle présentée par le promoteur ou le soumissionnaire en réponse à la DP.
Répondant	La personne ou l'entité (ou, dans le cas d'un consortium, les personnes ou les entités) qui présenteront une réponse à la suite de la présente IQ.
Réponse	Réponse officielle présentée par un Répondant au gouvernement du Canada à la suite de la présente IQ.
Reprise après sinistre (RAS)	Capacité d'une organisation de réagir à des événements considérables qui entraînent l'impossibilité temporaire pour l'organisation de fonctionner normalement. En ce qui concerne les systèmes et les services opérationnels essentiels hébergés, la RAS intègre des capacités particulières de réduction de la perturbation des services grâce à l'inclusion, par exemple, d'une protection des services de centres de données par la conservation hors région et dans divers centres au moyen de technologies de reproduction telles que la reproduction sur plateforme et la reproduction de stockage asynchrone.
Services	Tous les services techniques et professionnels fournis conformément au contrat qui découlera de la présente. Ceux-ci doivent inclure, sans s'y limiter, les services requis pour : 1. planifier, concevoir, installer, configurer, essayer, rendre opérationnel et appuyer le projet durant la période de l'entente; 2. offrir de la formation et de la documentation en ce qui concerne le projet; 3. permettre l'exploitation permanente du projet avant et après son acceptation par le Canada; 4. offrir des services de transition de sortie et de clôture du contrat, quelle que soit la raison pour laquelle la nécessité de la transition survient.
SGIPAE principal	En tant que produit offert sur le marché, une solution logicielle intégrée qui offre au moins les capacités fonctionnelles suivantes dans sa version commerciale : [gestion des nouveaux dossiers; gestion des cas; gestion des fournisseurs de services; gestion des aiguillages; gestion des rapports; gestion des utilisateurs; gestion des finances; gestion du portail]
Solution	L'ensemble de tous les produits et de tous les services de mise en œuvre envisagés selon les exigences énoncées dans l'énoncé des besoins pertinents ou dans un énoncé des besoins préparé par le Canada au sujet d'une exigence opérationnelle particulière, lesquels produits et services sont fournis conformément à la proposition technique et financière indiquée par le soumissionnaire dans la réponse écrite qu'il a présentée en réponse à une IQ, à une DDS ou à une invitation ou demande du même ordre.
Solution intégrée	Solution logicielle qui, bien que pouvant comprendre deux ou plusieurs modules (p. ex. géolocalisation, établissement de rapports, gestion des relations avec la clientèle, portail) et sans incidence sur le caractère fonctionnel, la fiabilité, la

Termes	Signification
	sécurité et la performance du système, offre l'expérience utilisateur de bout en bout d'une seule application.
Solution logicielle	Suite de produits logiciels requis pour satisfaire aux exigences, définis dans l'énoncé des besoins pertinent. La solution logicielle proposée peut consister en un produit logiciel auquel on a ajouté des modules d'extension de sorte qu'il satisfasse à des exigences fonctionnelles particulières; elle peut aussi consister en une suite intégrée de fonctions (produits) essentielles et complémentaires d'environnement de type portail ou d'une autre combinaison de produits logiciels qui, ensemble, permettent de satisfaire aux exigences. La solution logicielle peut constituer l'ensemble ou une partie de la solution fournie.
Soumissionnaire retenu	Soumissionnaire sélectionné par le Canada à l'issue du processus de la DDS et recommandé pour l'attribution du contrat.
Sous-traitant	Une entité avec laquelle un fournisseur a une relation contractuelle directe en vue de la réalisation d'une partie des travaux prévus au contrat conclu entre l'entrepreneur et le Canada; cela exclut les entités qui fournissent uniquement des biens commerciaux à l'entrepreneur.
Système	Terme générique utilisé pour désigner un réseau et d'autres dispositifs, systèmes d'exploitation, plateformes informatiques, logiciels de virtualisation et applications, ou une combinaison de ces éléments. Le sens du terme dépend du contexte.
TPSGC	Travaux publics et Services gouvernementaux Canada, aussi connu sous le nouveau nom de Services publics et Approvisionnement Canada (SPAC)
Travail	Toutes les activités, tous les services, tous les biens, tout l'équipement, toutes les matières et toutes les choses qui doivent être fabriqués, livrés ou réalisés par l'entrepreneur selon le contrat.
Unité opérationnelle	Une unité organisationnelle au sein d'une entreprise (p. ex. : une division ou une unité au sein de l'organisation du soumissionnaire) ou une société (p. ex. : un sous-traitant spécialisé) qui constitue un point de contact pour l'apport de compétences ou d'une expertise spécialisées dans un secteur d'activité, un secteur de prestation de services ou au sein de services d'infrastructure cibles. Les compétences, les services et l'expertise peuvent être démontrés par l'énumération d'atouts propres à un sujet au sein de l'unité ou de la société, et les atouts peuvent être entre autres des personnes, des processus et des technologies et infrastructures potentiellement particulières qui offrent des capacités accrues dans le secteur d'activité cible.
Utilisateur final	Employé interne ou partie externe qui s'est vu octroyer l'accès à l'application en tant qu'utilisateur.

Annexe B

Ébauche d'énoncé des besoins

Relatifs à la prestation d'un

Système de gestion de l'information pour le Programme d'aide aux employés

De la division des

Services d'aide aux employés (SAE)
de Santé Canada

Note : **La présente ébauche d'énoncé des besoins est une version simplifiée de l'énoncé des travaux à venir. Une version détaillée de l'énoncé des besoins sera fournie lors de l'invitation à soumissionner qui sera publiée dans le cadre du processus d'approvisionnement.**

TABLE DES MATIÈRES

1 INTRODUCTION

Le présent énoncé des besoins dresse la liste des besoins de haut niveau relatifs à la prestation d'un système de gestion de l'information pour le Programme d'aide aux employés qui permettra de répondre aux besoins de la Division des services d'aide aux employés (SAE) de Santé Canada.

La Division des SAE fait partie de la Direction des services de santé spécialisés (DSSS) de Santé Canada et offre en tout temps des services de consultation confidentiels, professionnels et bilingues. Elle se compose de près de 1 000 conseillers travaillant en cabinet privé partout au pays et aide près de 1,6 million de clients admissibles (employés et membres de la famille) de plus de 80 ministères et organismes fédéraux, y compris les Forces armées canadiennes, la Gendarmerie royale du Canada et les Anciens Combattants. La Division des SAE est le plus grand fournisseur de ce type de services au sein de la fonction publique fédérale.

La présente approche en matière d'approvisionnement a pour objectif de choisir un fournisseur qualifié qui offrira un système de gestion de l'information pour le Programme des services d'aide aux employés (PSAE) et des services connexes de mise en œuvre et de soutien pour répondre aux besoins de la Division des services d'aide aux employés de Santé Canada.

Dans le présent énoncé des besoins :

1. la section 1 présente un aperçu des objectifs et de la portée du projet;
2. la section 2 présente un aperçu de l'actuel PSAE de Santé Canada pour mettre en contexte la présente opportunité;
3. la section 3 présente la portée préliminaire de l'environnement du système de gestion de l'information du programme d'aide aux employés (SGIPAE) en mettant l'accent sur les exigences fonctionnelles, non fonctionnelles et de déploiement, l'environnement cible de bout en bout et les éléments fournis par le Canada et ceux devant être fournis par l'entrepreneur;
4. la section 4 présente le calendrier préliminaire associé à la transition de l'actuelle solution des SAE vers le nouveau SGIPAE fourni par l'entrepreneur choisi.

1.1 Objectifs du projet

Le projet a pour objectif d'obtenir et de mettre en œuvre un système de gestion de l'information pour le Programme des services d'aide aux employés qui permet d'accomplir ce qui suit :

1. fournir et déployer une solution logicielle qui répond aux besoins opérationnels fonctionnels, non fonctionnels et de sécurité ainsi qu'aux autres besoins précisés dans le présent énoncé des besoins;

2. déployer et opérationnaliser la solution dans les délais établis dans le calendrier principal du projet présenté à la section 4 du présent énoncé des besoins;
3. relever les défis associés à l'actuel environnement, notamment :
    a. garantir une disponibilité et une performance élevée,
    b. garantir une facilité d'utilisation pour les utilisateurs débutants et expérimentés qui utilisent le système chaque jour lors de situations stressantes,
    c. offrir des données de grande qualité provenant de diverses sources auxquelles les utilisateurs ont accès sans avoir à déployer trop d'efforts (qualité des données),
    d. offrir une solution facile à utiliser et grâce à laquelle il est facile d'ajouter, de supprimer ou de modifier les champs et les valeurs d'un menu déroulant, etc. afin de s'adapter au changement de l'environnement de travail (souplesse du système),
    e. mettre en œuvre une solution dont la portée peut facilement être élargie ou réduite (adaptabilité),
    f. garantir une efficacité opérationnelle,
    g. garantir la confidentialité des clients.

Le nouveau système permettra d'atteindre cinq objectifs **stratégiques** :

1. Permettre l'application d'une approche intégrée pour toutes les activités opérationnelles s'inscrivant dans la portée du système, soit :
    a. fonctions d'admission, de renvoi, de gestion de cas et d'assurance de la qualité,
    b. activités de gestion, comme la surveillance de la charge de travail et la surveillance des risques, qui appuient les fonctions mentionnées au point a. ci-dessus,
    c. protocoles appropriés d'accès des utilisateurs pour assurer un accès « aux personnes qui ont besoin de savoir » pouvant être établis à l'interne par l'entremise de niveaux d'accès et de délégation « superutilisateurs » ou « administrateurs »,
    d. interactions sur le Web sécurisées au moyen d'un portail dédié de fournisseurs de services affiliés pour la prise de rendez-vous, les renvois et la facturation;
2. Offrir une souplesse suffisante au personnel des SAE (selon le rôle) afin d'adapter les champs, les formulaires et les rapports sans avoir besoin de recourir à un codage personnalisé;
3. Favoriser une déclaration des résultats presque en temps réel (plus généralement : utilisation des services par les ministères et organismes, diverses

données démographiques, évaluations des résultats);

4. Favoriser une analyse améliorée en fonction des utilisateurs pour mieux orienter le processus décisionnel quant aux secteurs pour lesquels les efforts d'amélioration (y compris les efforts opérationnels et promotionnels) seraient les plus bénéfiques;
5. Disposer de la capacité inhérente d'adapter la solution de façon verticale (augmentation du volume et du revenu de l'entreprise) et horizontale (p. ex. nombre accru d'analyses et de rapports sur les données) à mesure que les SAE évolueront en tant que fournisseur de services.

Une fois ces objectifs stratégiques atteints, les gestionnaires de services, les fournisseurs de services affiliés, les conseillers, les spécialistes de gestion des cas et le bureau opérationnel des SAE utiliseront le SGIPAE afin d'accomplir ce qui suit :

1. recevoir, trier et renvoyer (c.-à-d. à un conseiller et à un fournisseur affilié) les demandes de services des comptes d'organisation et des membres de la famille;
2. gérer (ce qui comprend la recherche, l'accès, le visionnement, la référence croisée, la manipulation, la modification et la sauvegarde des modifications) les « dossiers » pour faciliter la coordination, l'administration, la surveillance et le suivi des services quotidiens (c.-à-d. réaliser toutes les activités de l'adhésion et à la facturation au moyen de la solution);
3. permettre l'identification, l'enregistrement et la déclaration d'indicateurs clés du rendement (ICR) définis par les utilisateurs;
4. permettre la comptabilité presque en temps réel pour la facturation et le paiement des fournisseurs de services affiliés;
5. permettre aux gestionnaires de surveiller la charge de travail de chaque spécialiste de gestion des cas et conseiller;
6. au moyen de repères temporels, s'assurer que les cas sont assignés ou ne deviennent pas dormants;
7. recueillir les renseignements personnels des employés du gouvernement fédéral (et des membres de leur famille), y accéder et les protéger;
8. favoriser la coordination efficace des activités et des communications entre les intervenants internes;
9. promouvoir l'uniformité et l'utilisation de pratiques exemplaires dans le cadre de la prestation de services d'aide aux employés et minimiser le fardeau administratif grâce à des normes de service intégrées; à la création automatique de notes de cas; à l'accès à des modèles de lettres et de formulaires et à l'accès direct à des directives en matière de SAE;
10. protéger les renseignements des employés du gouvernement fédéral afin que seuls les utilisateurs du système possédant les droits pertinents puissent avoir accès à ces renseignements;

11. facilement cerner les tendances relatives aux enjeux et aux lacunes et guider les modifications apportées aux pratiques et aux stratégies relatives aux SAE;
12. surveiller et évaluer le rendement du PAE au moyen de tableaux de bord et de la création de rapports préremplis et personnalisés à partir du poste de travail de l'utilisateur.

1.2 Portée des besoins

L'entrepreneur doit fournir un SGIPAE et des services connexes selon ce qui suit :

1. le SGIPAE doit offrir toute la gamme de fonctions opérationnelles des SAE, tel qu'il est indiqué à la section 3.2 du présent énoncé de besoins et précisé dans le cadre du processus d'approvisionnement;
2. le SGIPAE doit être déployé sur les services d'infrastructure fournis par le gouvernement du Canada, tel qu'il est indiqué dans la pièce jointe A du présent énoncé des besoins et précisé dans le cadre du processus d'approvisionnement;
3. les services sont fournis pour la conception, la configuration, l'intégration, le déploiement, la transition et le soutien continu du SGIPAE fourni et la transition éventuelle vers une autre solution ou d'autres services indiqués à la section 3.3 du présent énoncé de besoins et précisé dans le cadre du processus d'approvisionnement;
4. le SGIPAE doit se conformer aux exigences canadiennes en matière de sécurité énoncées aux annexes D, E et F de l'IQ et précisées dans le cadre du processus d'approvisionnement.
5. le SGIPAE doit se conformer aux exigences d'accessibilité défini dans la norme sur l'accessibilité des sites Web du gouvernement du Canada indiqués à la section 3.4 du présent énoncé de besoins et précisées dans le cadre du processus d'approvisionnement.

2 MODÈLE ACTUEL DES SAE

2.1 Aperçu du programme

Les Services d'aide aux employés (SAE) de Santé Canada gèrent le Programme d'aide aux employés (PAE) et offrent des services connexes aux organismes, aux ministères et aux organisations réglementées par le gouvernement fédéral, y compris les Forces armées canadiennes, la Gendarmerie royale du Canada et les Anciens Combattants.

Les SAE offrent ce qui suit :

1. Programme d'aide aux employés (PAE);
2. Services organisationnels spécialisés (SOS);
3. Gestion informelle des conflits (GIC);
4. Gestion des traumatismes;
5. Mesures et interventions d'urgence psychosociales (MIUP) ;
6. Gestion du stress professionnels ou d'incidents critiques (GSPIC).

Le Programme d'aide aux employés (PAE) est l'un des services offerts par les SAE. Entièrement accrédité par le Council on Accreditation (COA) Conseil d'accréditation (CA), le PAE répond à plus de 77 000 appels et a traité près de 29 200 cas pendant l'exercice 2018-2019. La demande en SAE devrait continuer d'augmenter au cours des prochaines années en raison de l'accent que met le greffier du Conseil privé sur les milieux de travail sécuritaires sur le plan physique et mental et des mesures que prennent les fonctionnaires publics, qui sont de plus en plus conscientisés aux enjeux relatifs à la santé mentale.

Le but du processus d'approvisionnement de SGIPAE est de choisir et de mettre en œuvre une nouvelle solution qui répond aux besoins opérationnels du PAE, simplifie les processus et tient compte de la Feuille de route de la Stratégie de données pour la fonction publique fédérale.

Pour cette majorité de ministères et d'organismes centraux, Santé Canada a un rôle direct à jouer pour aider leurs employés (et les membres de leur famille) à maintenir et à améliorer leur santé et mieux-être mental, dont les avantages directs comprennent ce qui suit : résilience accrue au stress et aux préjudices associés au stress opérationnel; productivité accrue au travail et réduction de l'absentéisme.

La Politique sur les résultats (en vigueur depuis le 1er juillet 2016) a renforcé les exigences des ministères et organismes pour définir et déclarer des indicateurs de résultats clairs. De plus, dans le respect des priorités du greffier du Conseil privé, la santé et le mieux-être mental au sein de la fonction publique (Stratégie pour la fonction publique fédérale sur la santé mentale en milieu de travail, en vigueur depuis le 28 novembre 2016) sont mis à l'avant, c'est-à-dire que les ministères doivent élaborer des plans d'action qui amélioreront la santé mentale générale au travail. Dans le cadre des efforts déployés pour adopter une approche pangouvernementale en matière de

mieux-être, la capacité de surveiller et de déclarer les résultats représente une exigence opérationnelle minimale.

En tenant compte de la portée des services fournis et de la croissance à venir (dans le contexte des cadres opérationnels fondés sur les résultats), l'adoption d'une solution qui répondra aux besoins actuels et futurs des SAE est importante sur le plan stratégique.

2.2 Technologies appuyant actuellement les SAE

À l'heure actuelle, plusieurs outils opérationnels sont utilisés pour appuyer la prestation du programme. Ces outils sont utilisés pour accomplir ce qui suit :

- gérer les admissions et les renvois du Centre d'intervention de crise et d'aiguillage ouvert 24 heures sur 24 (CICA – plus de 400 appels par jour);
- mener des activités de gestion des cas;
- gérer les coordonnées des clients, y compris les directives relatives à la facturation destinées à toutes les organisations clientes;
- recruter et gérer un réseau national d'environ 1 000 fournisseurs de services actifs;
- assurer aux gestionnaires des SAE un accès aux renseignements à jour des clients (directives spéciales, admissibilité des clients, services fournis, limites, etc.);
- assurer le suivi des plaintes et gérer les problèmes d'assurance de la qualité;
- générer des données sur l'utilisation qui sont fournies aux organisations des SAE;
- gérer les coordonnées des principales personnes-ressources (comptes d'organisation, représentants de l'organisme, fournisseurs de services affiliés);
- produire des rapports de gestion sur une base régulière ou sur demande;
- assurer le suivi des renseignements au sujet des besoins et des demandes de services;
- assurer le suivi des données financières.

Les composantes clés de l'actuel système d'information ont été conçues et tenues à jour au moyen de Lotus Notes. FileMaker, une plateforme de développement d'applications, a été utilisé pour répondre à certains besoins de la Division.

Des lacunes en matière de fonctionnalité et l'évolution des secteurs de service ont également demandé la mise en place de solutions de rechange et de processus manuels pour répondre à divers besoins. Le diagramme ci-dessous (figure 2.2-1) présente un aperçu des systèmes et des applications utilisés par les SAE pour offrir le PAE. De plus amples renseignements sont présentés dans le tableau 2.2-1.

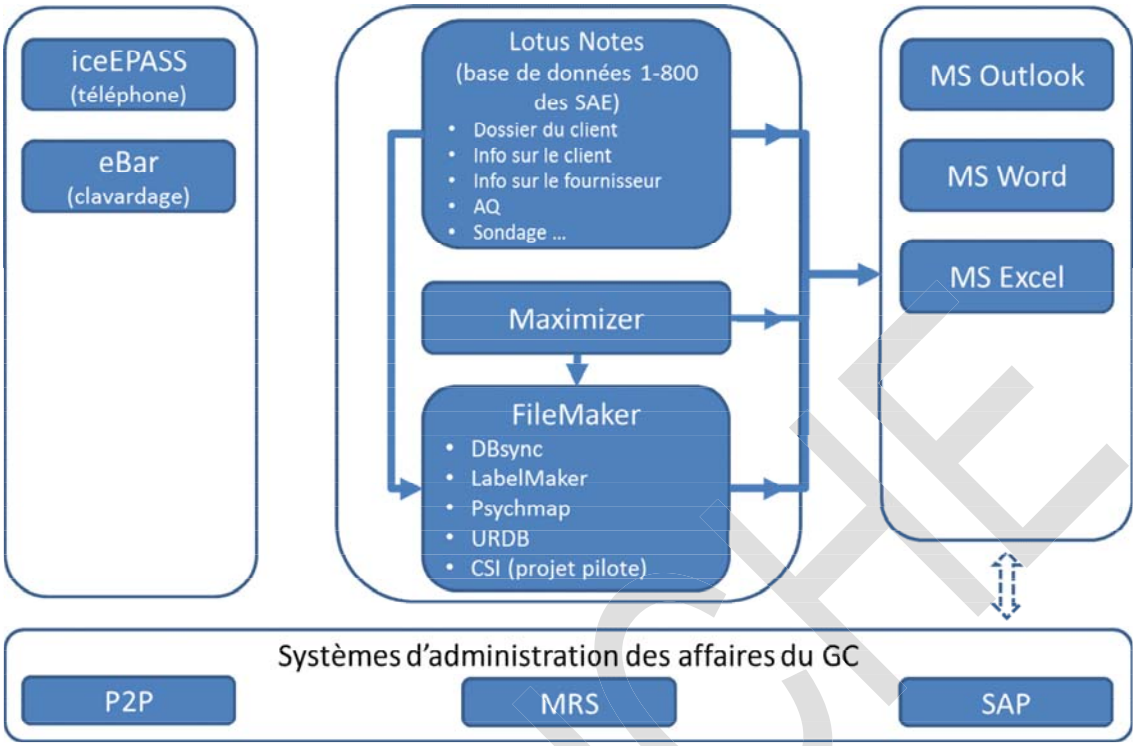

Figure 2.2-1 : Système actuel des SAE

Tableau 2.2-1 : Technologies appuyant actuellement les SAE

Système ou interface	Description
Base de données Lotus Notes	Une solution commerciale a été utilisée pour créer la version actuelle de l'application 1-800 des SAE pour répondre aux besoins du Programme d'aide aux employés offert par les SAE. Consigne et gère les clients, les cas, les études et les renseignements statistiques pertinents dans le cadre du PAE. Les données recueillies du numéro 1-800 des SAE s'alimentent dans les applications de déclaration créées dans FileMaker.
Maximizer	Solution commerciale de gestion des relations avec les clients. Deux bases de données assurent le suivi des renseignements des fournisseurs de services et des comptes d'organisation. Maximizer est utilisé pour ajouter des champs dans les modèles MS Word des extrants et des marchés formatés.

Système ou interface	Description
DBsync	Application bâtie sur la plateforme FileMaker pour comparer les données de plusieurs bases de données contenant des ensembles de données en double afin de cerner les lacunes et corriger les erreurs des données sources.
LabelMaker	Application bâtie sur la plateforme FileMaker pour créer des étiquettes papier pour les dossiers, comme les dossiers de facturation des fournisseurs de services (plus de 700 par année) et des étiquettes pour les grands envois. Les étiquettes peuvent être formatées de sorte à inclure certains renseignements, comme la région, le codage géographique et l'exercice financier.
PsychMAP	Application bâtie sur la plateforme FileMaker pour aider les utilisateurs à trouver un fournisseur de services par géolocalisation (latitude et longitude). Pour le PAE, les données sont importées de la base de données 1-800 Lotus Notes. PsychMAP est également utilisé en tant que principal outil de gestion des fournisseurs de services pour le groupe responsable des services organisationnels spécialisés (SOS).
URDB	Application bâtie sur la plateforme FileMaker pour générer des rapports d'utilisation des clients ainsi que des données d'utilisation des processus qui seront incluses dans divers rapports (rapport annuel et plan de programme, rapports budgétaires, rapports sur les coûts de consultation, rapports sur l'assurance de la qualité, etc.). L'application gère les configurations de rapports enregistrées par compte, la génération de rapports en lot et l'enregistrement de données regroupées.
CSI	Application bâtie sur la plateforme FileMaker pour faciliter la consignation de données des fournisseurs de services et les activités d'établissement de rapports. CSI normalise la consignation des données, s'assure que toutes les données sont valides avant leur soumission, génère des factures selon les renseignements consignés, gère les demandes de prolongation et le temps autorisé par cas et contribue au suivi du statut des paiements. Les factures sont générées en format HTML (texte brut) afin qu'elles soient soumises aux SAE dans un format non exclusif.

Système ou interface	Description
MS Outlook	Solution commerciale utilisée pour communiquer avec les autres par courriel, pour faire le suivi des tâches et des contrats et pour organiser des réunions et des présentations.
MS Word	Solution commerciale utilisée pour créer et modifier des documents. Exemples de documents créés par les SAE au moyen de MS Word : marchés, modèles de lettres, formulaires, lettres et rapports manuels.
MS Excel	Solution commerciale utilisée pour analyser des données et faire le suivi du statut.
SAP	Système financier du gouvernement du Canada utilisé pour consigner les données financières et en assurer le suivi (revenus et dépenses) et générer des paiements aux fournisseurs de services.
FileMaker	Plateforme commerciale de développement d'applications utilisée pour créer des applications internes afin d'automatiser des processus, d'augmenter la qualité du produit final et d'assurer l'utilisation efficace de ressources.

2.3 Intervenants du programme

En plus des employés du gouvernement demandant de l'aide, divers intervenants participent à la prestation de programmes et de services d'aide aux employés. Ces intervenants comprennent notamment un portefeuille de fournisseurs de services fournissant des services aux employés demandant de l'aide et divers intervenants responsables de l'administration, de la gestion et de la surveillance, qui assurant le bon fonctionnement des programmes et services. La figure 2.3-1 illustre la portée et le contexte des intervenants et leur interaction avec les systèmes et les solutions. Les tableaux 2.3-1 et 2.3-2 présentent plus de détails au sujet des intervenants et de leurs fonctions.

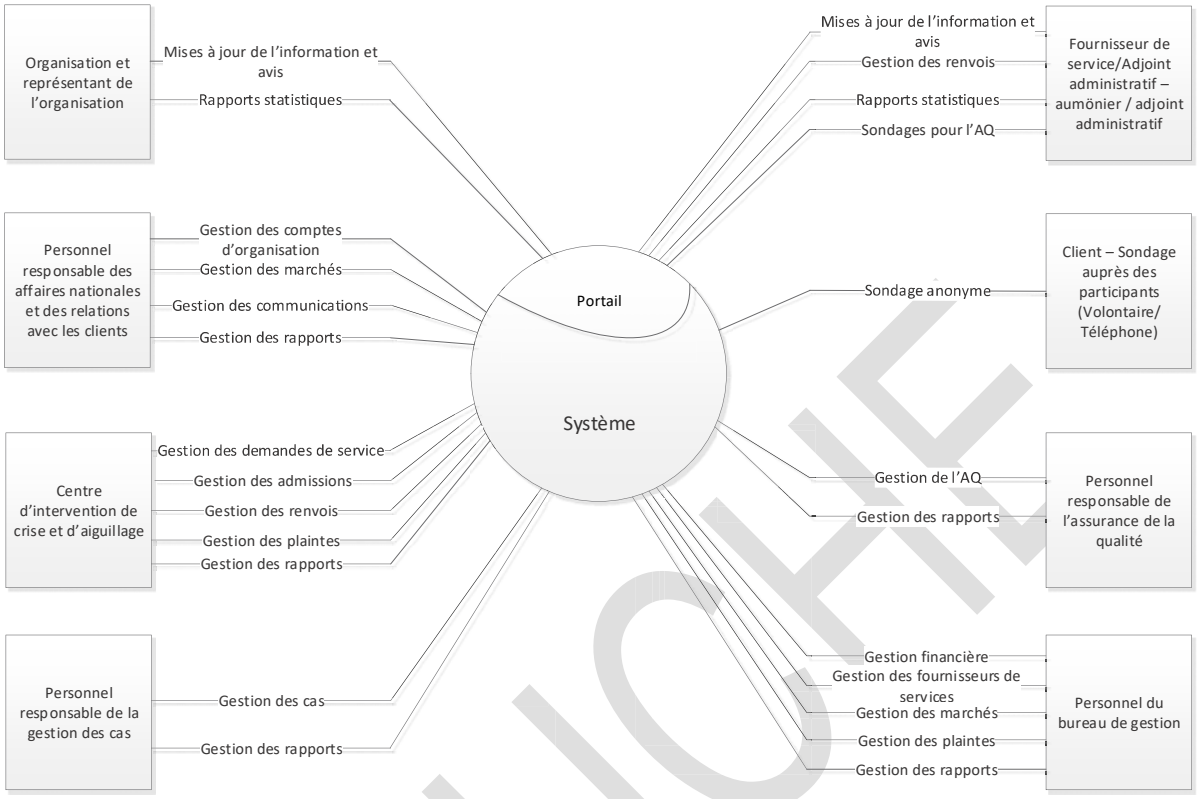

Figure 2.3-1 : Contexte opérationnel des intervenants du PAE

Tableau 2.3-1 Intervenants externes du PAE

Type d'intervenants	Description	Responsabilités	Nombre approximatif d'intervenants
Fournisseur de services	Un fournisseur de services est une personne qui fournit des services à des comptes d'organisation des SAE et aux SAE directement (p. ex. les SAE demandent au fournisseur de services de créer du matériel, des documents, des présentations, etc. au nom des SAE). Les intervenants profiteraient d'une gestion des contrats simplifiée (création et modification), ainsi que d'un suivi du temps et d'un traitement des factures plus simples.	Fournir des services aux clients qui ont été demandés et respecter les budgets établis. Soumettre les documents requis aux SAE.	800
Adjoint administratif du fournisseur de services	Un adjoint administratif du fournisseur de services est une personne qui travaille pour un fournisseur de services. Les intervenants profiteraient d'une gestion des contrats simplifiée (création et modification), ainsi que d'un suivi du temps et d'un traitement des factures plus simples.	Aider le fournisseur de services à respecter ses engagements contractuels d'un point de vue administratif.	200
Aumônier	Aumônier militaire pouvant fournir des services de consultation offerts par les SAE aux vétérans et à leur famille. Ces intervenants sont traités comme des entrepreneurs « réguliers ».	Offrir des services de consultation aux clients qui ont un lien avec le milieu militaire.	30

Type d'intervenants	Description	Responsabilités	Nombre approximatif d'intervenants
Client / Client organisationnel	Un client organisationnel est une entité fédérale, comme un ministère ou un organisme fédéral, une société d'État ou une organisation réglementée par le gouvernement fédéral, représentant l'ensemble de l'organisme ou une partie de l'organisme avec lequel les SAE ont conclu des marchés. Inclus aussi les Forces armées canadiennes, la Gendarmerie royale du Canada et les Anciens Combattants. Les utilisateurs n'interagissent pas directement avec le système.	Encourager les employés à utiliser les services des SAE qu'ils ont demandé aux SAE et permettre le paiement des frais	100
Représentant de l'organisme client	Un représentant d'organisme est un représentant qui possède des pouvoirs financiers de signer pour conclure des contrats de service avec le PAE au nom de cet organisme.	Agir en tant que personne-ressource principale pour le gestionnaire des clients des SAE et assurer la communication entre les SAE et le représentant de l'organisme.	125
Personne-ressource principale de l'organisme	La personne-ressource principale de l'organisme est la principale personne-ressource du client organisationnel qui répond aux questions sur le PAE. Les utilisateurs n'interagissent pas directement avec le système.	Assurer une communication adéquate entre le gestionnaire des comptes des SAE et les intervenants du compte de l'organisation.	200

Type d'intervenants	Description	Responsabilités	Nombre approximatif d'intervenants
Fournisseur de services d'entrevue téléphonique	Un fournisseur de services d'entrevue téléphonique est un fournisseur auquel font appel les SAE pour mener des entrevues téléphoniques avec les utilisateurs des SAE afin de déterminer leur niveau de satisfaction à l'égard des services qu'ils reçoivent. Les utilisateurs du PAE avec qui le fournisseur communique ont déjà accepté de participer au sondage. Les utilisateurs n'interagissent pas directement avec le système.	Effectuer des entrevues téléphoniques avec les utilisateurs du PAE, consigner les résultats et diffuser l'information regroupée à l'équipe des SAE.	1
Client	Un client est une personne qui appelle pour demander des services du PAE. Le client peut être autorisé à accéder au PAE en fonction de critères établis pour son organisme ou peut être un demandeur non qualifié. Les clients qualifiés du PAE sont généralement des employés ou des personnes qui ont un lien avec un employé d'un organisme gouvernemental fédéral, d'un ministère ou d'un organisme fédéral, d'une société d'État ou d'un organisme réglementé par le gouvernement fédéral, y compris les Forces armées canadiennes, la Gendarmerie royale du Canada et les Anciens Combattants. Les clients peuvent également être des participants au sondage.	Utiliser le PAE de la manière prévue	25 000

Type d'intervenants	Description	Responsabilités	Nombre approximatif d'intervenants
	Les clients bénéficieraient indirectement d'un système que le conseiller du CICA peut utiliser avec facilité puisque l'expérience serait ainsi plus fluide.		
Demandeurs	Toute personne qui communique avec le PAE.		70 000

Tableau 2.3-2 Intervenants internes du PAE

Type d'intervenants	Description	Responsabilités	N^{bre} approximatif d'intervenants
Centre d'intervention de crise et d'aiguillage (CICA)			
Coordonnateur de la logistique du CICA	Coordonne les activités des conseillers du CICA. Coordonne et offre de la formation. Remplace le superviseur du CICA au besoin. Profiterait d'un système facile à utiliser, au sujet duquel il pourrait offrir une formation aux autres et qui est accompagné d'une bonne documentation. Ce système devrait également être capable de générer des rapports de gestion.	Coordonner les activités des conseillers, offrir des séances de formation et remplacer le superviseur du CICA, au besoin.	1
Gestionnaire des services de consultation et d'assurance de la qualité (AQ)	Gère l'équipe de gestion des cas et le superviseur de l'AQ. Reçoit des avis d'incidents traumatiques par l'entremise du groupe responsable des traumatismes des SAE (compte de courriels générique). Souhaiterait pouvoir générer facilement différents types de rapports de gestion et analyser différents facteurs. Voudra s'assurer que le système peut s'adapter à différents types de scénarios et que les conseillers du CICA peuvent fournir facilement l'information nécessaire aux clients en détresse. Doit être capable de voir les dossiers des clients au	Superviser la gestion et la prestation de services de consultation.	1

Type d'intervenants	Description	Responsabilités	Nbre approximatif d'intervenants
	besoin. Utilise tous les aspects du système.		
Superviseur du CICA	Supervise le CICA et ses opérations en tout temps. S'assure que les services sont offerts conformément aux directives établies et dans le respect des normes de qualité et intègre le volet de supervision clinique. Utilise souvent les composantes opérationnelles et de prestation de services du système. Souhaite disposer d'une solution pour les conseillers du CICA facile à utiliser, offre des fonctions intégrées, mais permet aux conseillers de consigner facilement des renseignements spéciaux qui ne sont pas encore des choix ou des options prédéterminés dans les menus déroulants. Veille à ce que les données et les renseignements sur la qualité soient consignés dans le système aux fins de suivi, de gestion et de surveillance.	Superviser les opérations du CICA pour veiller au respect des critères établis.	1
Conseiller du CICA	Premier point de contact des clients du Programme d'aide aux employés qui ont besoin de services d'aide ou d'autres services psychosociaux. Principal utilisateur du système. Recueille de l'information pour évaluer si des services de consultation ou psychosociaux sont requis et intervenir en conséquence. Si un tel service est requis, ouvrir un cas et diriger le client vers un fournisseur de services. Certains conseillers travaillent à distance et se déconnectent parfois d'Internet.	Répondre aux appels des clients, prendre les mesures nécessaires et remplir les documents requis aux fins de gestion.	12
Adjoint administratif du CICA	Principal utilisateur des fonctions d'administration du système.	Fournir un soutien administratif aux conseillers du CICA	3

Type d'intervenants	Description	Responsabilités	Nbre approximatif d'intervenants
	Fournit des renseignements sur les cas du PAE aux fournisseurs de services, met à jour les disponibilités des fournisseurs de services et répond à d'autres besoins en matière d'information. Consigne toutes les demandes de prolongation des fournisseurs de service (y compris leurs plans) dans le système et fournit des données statistiques aux gestionnaires de cas. Assume des fonctions de vérification pour assurer l'intégrité des données. Souhaiterait être capable de mettre à jour facilement les données, à les trouver et à les extraire.	et à l'équipe de gestion des cas.	
Coordonnateur de la logistique du CICA	Coordonne les activités des conseillers du CICA. Coordonne et offre de la formation. Remplace le superviseur du CICA au besoin. Profiterait d'un système facile à utiliser, pour lequel il pourrait offrir une formation aux autres et possède une bonne documentation. Ce système devrait également être capable de générer des rapports de gestion.	Coordonner les activités des conseillers, offrir des séances de formation et remplacer le superviseur du CICA, au besoin.	1
Gestionnaire des services de consultation et d'assurance de la qualité (AQ)	Gère l'équipe de gestion des cas et le superviseur de l'AQ. Reçoit des avis d'incidents traumatiques par l'entremise du groupe responsable des traumatismes des SAE (compte de courriels générique). Souhaiterait pouvoir générer facilement différents types de rapports de gestion et analyser différents facteurs. Voudra s'assurer que le système peut s'adapter à différents types de scénarios et que les conseillers du CICA peuvent fournir facilement l'information nécessaire aux clients en détresse. Doit être capable de voir les dossiers des clients au	Superviser la gestion et la prestation de services de consultation.	1

Type d'intervenants	Description	Responsabilités	Nbre approximatif d'intervenants
	besoin, Utilise tous les aspects du système.		
Superviseur du CICA	Supervise le CICA et ses opérations en tout temps. S'assure que les services sont offerts conformément aux directives établies et dans le respect des normes de qualité et intègre le volet de supervision clinique. Utilise souvent les composantes opérationnelles et de prestation de services du système. Souhaite disposer d'une solution pour les conseillers du CICA facile à utiliser, offre des fonctions intégrées, mais permet aux conseillers de consigner facilement des renseignements spéciaux qui ne sont pas encore des choix ou des options prédéterminés dans les menus déroulants. Veille à ce que les données et les renseignements sur la qualité soient consignés dans le système aux fins de suivi, de gestion et de surveillance.	Superviser les opérations du CICA pour veiller au respect des critères établis.	1
Conseiller du CICA	Premier point de contact des clients du Programme d'aide aux employés qui ont besoin de services d'aide ou d'autres services psychosociaux. Principaux utilisateurs du système. Recueille de l'information pour évaluer si des services de consultation ou psychosociaux sont requis et intervenir en conséquence. Si un tel service est requis, ouvre un cas et dirige le client vers un fournisseur de services. Certains conseillers travaillent à distance et se déconnectent parfois d'Internet.	Répondre aux appels des clients, prendre les mesures nécessaires et remplir les documents requis aux fins de gestion.	12
Adjoint administratif du CICA	Principal utilisateur des fonctions d'administration du système.	Fournir un soutien administratif aux conseillers du CICA	3

Type d'intervenants	Description	Responsabilités	N^bre approximatif d'intervenants
	Fournit des renseignements sur les cas du PAE aux fournisseurs de services, met à jour les disponibilités des fournisseurs de services et répond à d'autres besoins en matière d'information. Consigne toutes les demandes de prolongation des fournisseurs de service (y compris leurs plans) dans le système et fournit des données statistiques aux gestionnaires de cas. Assume des fonctions de vérification pour assurer l'intégrité des données. Souhaiterait être capable de mettre à jour facilement les données, à les trouver et à les extraire.	et à l'équipe de gestion des cas.	
Gestion des cas (GC)			
Spécialiste de gestion des cas (SGC)	Autorise ou refuse les demandes de prolongation des fournisseurs de services pour d'autres séances en fonction de leur requête. Collabore avec les fournisseurs de services afin de cerner les stratégies pertinentes pour assurer un bon suivi des cas. Appuyer les fonctions opérationnelles liées au paiement des fournisseurs de services.	Examiner les demandes de prolongation et approuver ou refuser les demandes en fonction de l'information fournie. Aider le bureau administratif en fournissant des documents relatifs aux paiements.	6
Adjoint administratif de l'équipe de gestion des cas (AAGC)	Procède à la vérification préliminaire des demandes de prolongation des fournisseurs de services. Approuve les demandes de prolongation standards et envoie les cas plus complexes au commis de gestion des cas. Consigne les renseignements sur les demandes de prolongation standards.	Gérer les demandes de prolongation et les activités de consultation.	1
Commis de gestion des cas (CGC)	Distribue les demandes de prolongation au SGC.	Veiller à la distribution des demandes de prolongation et au	1

Type d'intervenants	Description	Responsabilités	N^bre approximatif d'intervenants
		suivi des demandes en attente.	
Assurance de la qualité (AQ)			
Superviseur de l'assurance de la qualité (SAQ) du PAE	Interagit avec les clients, les fournisseurs de services et les intervenants du PAE. Étudie les plaintes des clients. Analyse les résultats des sondages et des examens périodiques. Coordonne et organise des séances d'orientation aux deux semaines pour les nouveaux conseillers du réseau. Fournit des rapports individuels détaillés sur chaque plainte reçue et consigne les données dans le système des SAE. Fournit à la haute direction des rapports mensuels sur toutes les plaintes reçues pendant un mois donné. Vérifier les cas de « non-conformité » pour assurer qu'ils ne se produisent pas de nouveau. A accès aux dossiers de plaintes d'un organisme (fermées et ouvertes), aux remarques sur l'assurance de la qualité et à des renseignements détaillés sur les fournisseurs de services.	Examiner les résultats des sondages et prendre les mesures nécessaires auprès des intervenants concernés pour s'assurer que les clients du PAE sont satisfaits des services reçus.	1
Adjoint administratif du superviseur de l'assurance de la qualité (AAAQ) du PAE	Gère les processus d'assurance de la qualité. Crée un rapport annuel comprenant, entre autres, le nombre de personnes ne s'étant pas présentées à leur rendez-vous, les clients « uniques », le nombre de sondages remplis, le nombre de nouveaux dossiers créés et le délai moyen avant le premier rendez-vous. Consigne les commentaires formulés dans le sondage volontaire. Gère la distribution du sondage volontaire.	Aider le superviseur de l'AQ en produisant des rapports et des documents pertinents.	1

Type d'intervenants	Description	Responsabilités	N^bre approximatif d'intervenants
Affaires nationales et relations avec les clients			
Gestionnaire national des affaires et des relations avec les clients	Supervise les activités des gestionnaires des clients des SAE. Extrait les rapports de gestion et documente les interactions avec les comptes d'organisation en détail	Promouvoir les services des SAE, le développement des entreprises et les relations avec les clients.	1
Gestionnaire des clients des SAE (GC)	Agit en tant que liaison avec les comptes d'organisation pour assurer de bonnes relations avec eux et leur satisfaction, négocier de nouveaux contrats et leur renouvellement et promouvoir tous les secteurs de services des SAE de façon continue. Examine les taux d'utilisation, mène des analyses et discute des résultats d'utilisation avec les comptes d'organisation.	Travailler avec les comptes d'organisation pour répondre à leurs besoins en services d'aide aux employés, y compris l'accès à un service du PAE.	4
Gestionnaire régional des clients des SAE	Même description de travail que les gestionnaires des clients des SAE, mais travaille à distance (c.-à-d. travaille dans les régions, ne se trouve pas physiquement dans la région de la capitale nationale).	Travailler avec les comptes d'organisation pour répondre à leurs besoins en services d'aide aux employés, y compris l'accès à un service du PAE.	2
Adjoint administratif des gestionnaires des clients des SAE (AAGC)	Offre une aide administrative aux gestionnaires des clients des SAE. Réalise des tâches opérationnelles quotidiennes liées au travail des gestionnaires des clients des SAE comme, préparer des factures pour la distribution, créer des modèles de lettres, tenir à jour des modèles de rapports, surveiller le site Web et les demandes d'information générées par l'entremise de celui-ci. Mettre à jour diverses listes. Important utilisateur du système.	Appuyer le travail des gestionnaires des clients des SAE en préparant les documents et les rapports pertinents.	2

Type d'intervenants	Description	Responsabilités	N^bre approximatif d'intervenants
Bureau de gestion (BG)			
Superviseur du bureau de gestion	Supervise tous les aspects du bureau de gestion. Coordonne la planification du budget et les rapports, la facturation aux comptes d'organisation et aux clients des SOS, le paiement des fournisseurs de services du PAE et des SOS. Gère les comptes débiteurs, les comptes créditeurs, l'achat, les rapports sur les écarts, la consignation des données financières, la création de marchés, etc.	Superviser et gérer tous les aspects du bureau de gestion.	1
Adjoint administratif du bureau de gestion (AABG)	Consigne l'information reçue des fournisseurs de services qui envoient des factures mensuelles et des statistiques, crée des appels pour les services des PAE et des SOS et tient à jour des tableaux de suivi et assume d'autres fonctions administratives.	Aider le superviseur du bureau de gestion à préparer les rapports et les documents pertinents.	1
Coordonnateur du réseau des conseillers (CRC)	Négocie les modalités des accords d'offre à commandes (AOC) et les consigne. Gère les renseignements et les documents sur les fournisseurs de services (contrôle de sécurité, attestation d'études, preuve d'assurance-responsabilité, certification professionnelle, etc.).	Évaluer, embaucher et gérer les fournisseurs de services du réseau du PAE.	2
Adjoint administratif du coordonnateur du réseau des conseillers (AACRC)	Crée et modifie les AOC pour les nouveaux fournisseurs de services et les fournisseurs existants. Crée et tient à jour les profils des fournisseurs de services. Crée des appels pour les projets de SOS.	Appuyer le réseau de coordonnateurs des services de consultation en préparant les rapports et les documents pertinents.	1
Commis à la consignation des données (CCD)	Vérifie les données dans les factures et les rapports statistiques connexes reçus des fournisseurs de services. Fait des suivis auprès des fournisseurs de services	Vérifier et consigner des données tirées des factures et des autres documents.	7

Type d'intervenants	Description	Responsabilités	N^bre approximatif d'intervenants
	lorsqu'aucune donnée statistique n'est reçue.		
Agent du service à la clientèle (ASC)	Aide les fournisseurs de services à accéder au portail externe des SAE. Met à jour le tutoriel en ligne, au besoin. Envoie des communications aux fournisseurs de services par courriel.	Appuyer les fournisseurs de services en ce qui a trait aux SAE.	1
Direction			
Directeur, Services d'aide aux employés	Responsable de tous les aspects de la division des SAE. Doit pouvoir accéder à toutes les données et à tous les rapports.	Gérer la division des SAE, y compris la mise en œuvre du PAE.	1

3 EXIGENCES PRÉLIMINAIRES CIBLES DU SGIPAE

3.1 Aperçu

Le modèle **cible** de déploiement du SGIPAE est présenté à la figure 3.1-1.

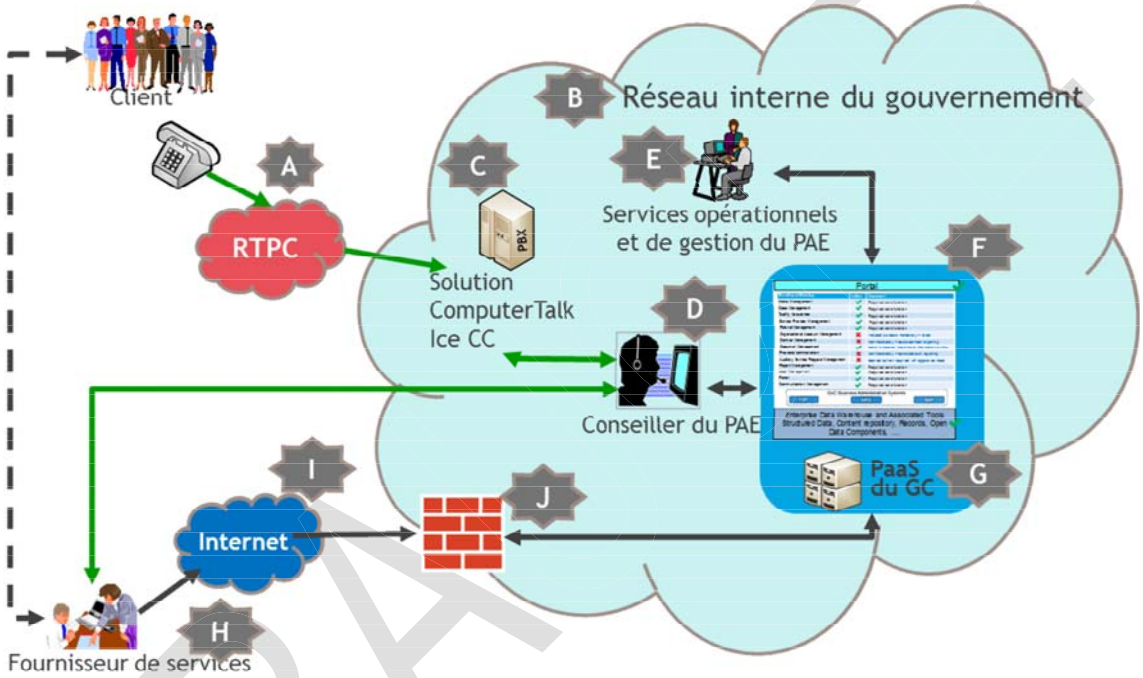

Figure 3.1-1 : Modèle cible de déploiement du SGIPAE de Santé Canada

Dans la figure 3.1-1

A	RTPC	Les clients ont accès aux services des SAE par l'entremise du système téléphonique commuté public et d'une fonction de clavardage. Il est possible d'accéder aux services vocaux au moyen d'un ensemble de numéros 1-800. Ces numéros sont liés au système de gestion des appels du centre d'appel du gouvernement (actuellement la solution ComputerTalk iceEPASS, configurée pour répondre à certaines exigences en ce qui a trait au traitement des appels du programme). La solution ComputerTalk iceEPASS n'est pas intégrée aux systèmes opérationnels (p. ex. plateforme de GRC). Dans le modèle cible, cette opération indépendante se poursuivra

		(c.-à-d. il n'est pas nécessaire d'intégrer iceEPASS au SGISAE).
B		Infrastructures du réseau de transmission de la voix et des données du gouvernement du Canada utilisées par tous les intervenants internes (au gouvernement) et offrant un accès sécurisé aux applications des SAE et aux données conservées dans les plateformes gérées par le gouvernement. Le réseau d'entreprise du gouvernement offre un niveau de sécurité, de redondance, de rendement, de capacité d'accès et d'accessibilité suffisant pour appuyer les intervenants internes.
C		Solution de gestion des appels du centre d'appels ComputerTalk iceEPASS configurée pour répondre aux exigences relatives au traitement des appels du programme. La plateforme iceEPASS gère les files d'appels entrants et n'est pas directement intégrée aux systèmes principaux (c.-à-d. aucune fenêtre contextuelle ou autre fonction automatisée de gestion des appels requise).
D		Conseiller des SAE de Santé Canada, qui agit en tant que premier point de contact pour les clients faisant appel aux SAE. Les conseillers en SAE utilisent des appareils informatiques et de voix conformes aux normes de Santé Canada et du gouvernement du Canada. Tous les conseillers des SAE font partie de l'infrastructure du gouvernement du Canada. Les conseillers hors site utilisent des appareils et de l'équipement du gouvernement du Canada pour accéder au réseau du gouvernement.
E		Les utilisateurs des fonctions opérationnelles et administratives des SAE offrent des services d'assurance de la qualité, de gestion des cas et d'administration pour gérer les programmes et les services des SAE. Les utilisateurs des fonctions opérationnelles et administratives des SAE utilisent des appareils informatiques conformes aux normes de Santé Canada et du gouvernement du Canada. Tous ces utilisateurs font partie de l'infrastructure du gouvernement du Canada.
F		Portefeuille des systèmes opérationnels des SAE essentiels pour répondre aux besoins opérationnels du programme énoncés dans le présent énoncé des besoins. Le portefeuille de systèmes doit être fourni dans divers environnements de déploiement du gouvernement du Canada sur les plateformes d'exploitation, environnements qui sont décrits dans le présent énoncé des besoins et comprenant notamment des environnements de production, de simulation, de mise à l'essai/de développement et de RS.

G	 PaaS du GC	Plateforme comme services (PaaS) fournis par le gouvernement du Canada et configurés pour répondre aux exigences non fonctionnelles et en matière de rendement, de capacité et de sécurité du SGIPAE qui sont requises pour atteindre les objectifs relatifs au niveau de service opérationnel. La plateforme comme services fournis par le gouvernement du Canada sera offerte pour appuyer les environnements de déploiement nécessaires indiqués dans le présent énoncé de besoins et comprenant notamment des environnements de production, de simulation, de mise à l'essai/de développement et de RS. La plateforme comme services du gouvernement du Canada sera conforme aux directives du Conseil du Trésor (CT) en matière de plateforme de services pouvant traiter des charges de travail de niveau Protégé B. La plateforme comme services du gouvernement du Canada sera configurée afin d'offrir un niveau approprié de disponibilité élevée et une fonction de RS afin de se conformer avec l'objectif de point de reprise (OPR) et l'objectif de temps de reprise (OTR) qui sont indiqués dans le présent énoncé des besoins.
H	 Fournisseur de services	Le fournisseur de services est un fournisseur externe indépendant (au gouvernement du Canada) de services d'aide aux employés. Un fournisseur de services est assigné aux clients par le conseiller en SAE. Selon les soins requis, une interaction directe se produit entre le client et le fournisseur pour la prestation de services. Tous les rapports et les dossiers sur les services d'aide aux employés sont conservés par le fournisseur de services. Les interactions entre le fournisseur de services et l'environnement de SAE du gouvernement du Canada ont pour objet la gestion et l'administration du programme.
I		Accès électronique au régime de gestion et d'administration du PAE du gouvernement du Canada par les intervenants externes, comme les fournisseurs de services, fourni par un accès Internet sécurisé. N'existe pas à l'heure actuelle – fait partie du « déploiement cible ».
J		Accès électronique au régime de gestion et d'administration des SAE du gouvernement du Canada par les intervenants externes, comme les fournisseurs de services, au moyen d'un accès Internet sécurisé contrôlé grâce à une configuration appropriée de services pare-feu sécurisés. N'existe pas à l'heure actuelle – fait partie du « déploiement cible ».

3.2 Exigences fonctionnelles opérationnelles du SGIPAE

Le SGIPAE intégré doit offrir les fonctions opérationnelles nécessaires pour répondre aux besoins du Canada qui sont indiqués dans l'énoncé des besoins. Plus précisément :

1. Le SGIPAE intégré doit répondre aux besoins suivants :
    a. gestion des inscriptions, comme indiqué à la section 3.2.1;
    b. gestion des cas, comme indiqué à la section 3.2.2;
    c. assurance de la qualité, comme indiqué à la section 3.2.3;
    d. gestion des fournisseurs de services, comme indiqué à la section 3.2.4;
    e. gestion des renvois, comme indiqué à la section 3.2.5;
    f. gestion des clients organisationnels, comme indiqué à la section 3.2.6;
    g. administration financière, comme indiqué à la section 3.2.9;
    h. gestion des rapports, comme indiqué à la section 3.2.11;
    i. gestion des utilisateurs, comme indiqué à la section 3.2.12;
    j. portail de services, comme indiqué à la section 3.2.13;
    k. gestion des communications, comme indiqué à la section 3.2.14.

3.2.1. Gestion des admissions

Le terme « gestion des admissions » désigne la capacité de recueillir et de gérer les renseignements des clients et de les gérer afin de fournir le service approprié. Le processus peut demander une consultation immédiate, un renvoi vers un fournisseur de services (FS), une évaluation des besoins ou le renvoi à un autre secteur de services internes.

- Assurer le suivi des appels des clients et les gérer.
- Associer un appel à un dossier de client, un nouveau cas ou un cas existant ou toute activité liée au cas, comme un renvoi, la diffusion d'information ou le renvoi à un autre secteur de services.
- Valider l'admissibilité du client à recevoir le service en accédant aux contrats ou ententes pertinentes.
- Évaluer les clients au moyen de documents de référence.
- Diriger le client vers un fournisseur de services (voir la section sur la gestion des renvois).

3.2.2. Gestion des cas

Le terme « gestion des cas » désigne le processus collaboratif d'évaluation, de planification et de coordination des soins pour répondre aux besoins des clients.

- Faire une recherche sur les clients, les antécédents du cas, les cas connexes, les paiements connexes et toutes les notes associées au dossier.
- Gérer les dossiers de cas, les renseignements et les stratégies de cas existants.

- Consigner les décisions et toutes les communications liées au cas avec un fournisseur de services.

3.2.3. Assurance de la qualité

L'« assurance de la qualité » consiste à repérer, à documenter, à saisir et à suivre les cas de non-conformité aux politiques des SAE et à l'information fournie par le client. Elle consiste également à gérer les plaintes, à assurer la confidentialité et à traiter les plaintes dans un délai raisonnable, soit en accusant réception de celle-ci et en documentant le processus résolution.

- Faire des visites sur place et des suivis auprès des fournisseurs de services
- Gérer les modèles de sondage
- Recueillir des données de sondage
- Repérer les cas de non-conformité et recueillir l'information fournie par le client
- Diverses sources possibles de plaintes – client, fournisseur de services, personne-ressource du client, etc.
- Examiner, enquêter et documenter
- Donner accès aux plaintes à un nombre restreint d'utilisateurs

3.2.4. Gestion des fournisseurs de services

La gestion des fournisseurs de services (FS) sert à surveiller la tenue à jour et le maintien de l'accréditation des fournisseurs de services, ainsi que les efforts de simplification du recrutement, et à rechercher et à analyser les réseaux.

- Créer et gérer le profil des fournisseurs de services
- Déterminer la santé du réseau de fournisseurs de services par secteur de service
- Accéder à tous les marchés conclus en vertu des offres à commandes pertinentes – par secteur de service
- Créer et gérer des marchés en vertu des offres à commandes (voir la section sur la gestion des contrats)
- Géocoder l'emplacement des bureaux
- Gérer les documents des fournisseurs de services (voir la section sur la gestion des documents)

3.2.5. Gestion des renvois

La gestion des aiguillages consiste à recenser les ressources des fournisseurs de services adéquats et à établir la communication avec le client ou l'organisme, et à suivre et gérer les communications menant à l'acceptation ou au refus de l'aiguillage.

- Consulter les renvois pour lesquels le fournisseur n'a pas rappelé pour obtenir les détails du renvoi

- Saisir les décisions des fournisseurs de services quant à l'acceptation ou au refus
- Suivre le temps écoulé avant la consultation des détails et assurer le suivi auprès du ou des fournisseurs de services
- Effectuer une recherche de géolocalisation

3.2.6. Gestion des clients organisationnels

La gestion des comptes d'organisation consiste à évaluer de façon constante les exigences liées au compte et à mettre à jour le profil du client en fonction des modifications qui s'imposent. La gestion des clients organisationnels a pour but de promouvoir les services psychosociaux par des communications directes ou des événements afin d'accroître le nombre de personnes en cause et garantir une communication réceptive et en temps opportun avec les clients organisationnels

- Créer et mettre à jour les organisations et les comptes d'organisation
- Gérer et créer des comptes associés aux marchés inscrits dans le système
- Suivre les communications liées aux comptes
- Saisir les commandes d'articles promotionnels

3.2.7. Gestion des marchés

La gestion des marchés désigne le processus de définition des ententes contractuelles, de gestion de l'état du marché, de gestion des modifications au marché et de la production de documents associés à un marché.

- Devoir appuyer divers types de marchés
- Créer des marchés et des modifications aux marchés. Dresser l'historique des ententes contractuelles.
- Gérer les dates actives, les modifications concernant les dates, les dates d'expiration et/ou d'autres modifications aux données pertinentes.
- Le document de modification du contrat devrait mentionner les modifications du contrat en vigueur par rapport au contrat précédent.
- Gérer l'état des contrats.
- Enregistrer les documents créés dans le dépôt de documents.
- Pouvoir créer des contrats dans la langue de préférence du récipiendaire (français et/ou anglais).
- Être capable de gérer les gabarits de contrats
- Passer des commandes (la passation comme telle d'une commande est effectuée dans SAP – voir la section sur la gestion financière).

3.2.8. Gestion des documents

La gestion de documents désigne le processus d'organisation, de stockage et de suivi des documents électroniques dans le dépôt central des documents.

- Rechercher les métadonnées associées aux documents (comme le type de sécurité, les dates d'expiration, la classification des documents, etc.).
- Gérer les documents périmés.
- Les documents doivent être codés conformément à l'algorithme cryptographique recommandé par le Centre de la sécurité des télécommunications (CST).

3.2.9. Gestion financière

La gestion financière consiste à faire payer les sommes dues et à facturer celles qui doivent être payées.

- Valider les lignes de la facture du fournisseur de services par rapport à la décision originale de renvoi et de gestion des dossiers (le cas échéant).
- Créer de nouvelles commandes en vertu d'une offre à commandes et tenir à jour les commandes existantes
- Lier chaque élément de service facturé par le fournisseur de services à la commande appropriée passée en vertu de la convention d'offre à commandes qui est en vigueur aux dates de service.
- Vérifier quelles commandes ont été utilisées pour payer des factures particulières.
- Permettre des modifications aux factures originales des fournisseurs de services, et en assurer le suivi.
- Créer une facture de fournisseur de services avec des avis de rajustement.
- Suivre les valeurs du contrat à rétrofacturer au compte d'organisation ou au client.
- Calculer les frais.
    - Calculer la somme à facturer au compte d'organisation ou au client en fonction des tranches de frais (définies dans le contrat ou le projet) et des sommes déjà facturées.
    - Pour les services facturés à l'utilisation pouvoir calculer la somme à facturer au compte ou au client en fonction des services fournis.

3.2.10. Gestion des demandes de service

La gestion des demandes de services consiste à exercer des fonctions de planification d'ordonnancement, de contrôle des coûts et de gestion du budget. Les utilisateurs peuvent ainsi gérer la prestation des services. Elle permet également d'assurer le suivi des activités de communication et d'assurance de la qualité.

- Évaluer et saisir les besoins des clients éventuels.
- Utiliser un mécanisme de recherche pour aider les utilisateurs à établir des prévisions de coût des services.
- Préciser la prestation de chaque service requis avec le lieu et la date.
- Soutenir la capacité de saisir et de visualiser une multitude de coûts calculés pour la prestation d'un service.
- Définir un ensemble de services en fonction des objectifs et des budgets des clients.
- Créer des propositions et citer des prix avec des prévisions de coût pour les clients éventuels.
- Créer des ententes de services, des lettres d'entente interministérielle, des protocoles d'entente et des marchés (voir la section sur la gestion des marchés).
- Gérer les interventions selon les dates et les heures.
- Constater et régler les conflits de réservations.

3.2.11. Gestion des rapports

La gestion des rapports permet la recherche et l'analyse de données. Il s'agit de définir d'avance les paramètres des rapports, d'exécuter un jeu de rapports types et de produire des rapports en grande quantité en pouvant les archiver dans un dépôt de documents avec un suivi possible par catégorie documentaire. La gestion des rapports devrait rendre anonymes ou non identifiables les données sensibles ou celles qui peuvent être rapportées à une seule personne ou porter préjudice à un groupe.

- Les utilisateurs peuvent configurer les paramètres des rapports.
- Le système doit pouvoir faire le suivi des configurations par compte organisationnel.
- La solution doit pouvoir soutenir la capacité de l'utilisateur à créer et à modifier des rapports.
- Les rapports liés aux clients doivent être versés dans un dépôt de documents.
- Il faut pouvoir gérer les modèles de rapports.
- Il faut pouvoir produire les rapports en PDF, DOCX ou Excel.
- Il faut pouvoir produire des rapports en lots.
- Il faut pouvoir produire des rapports complexes (données venant de sources d'information multiples, internes et/ou externes).

3.2.12. Gestion des utilisateurs

La gestion des utilisateurs permet de créer et de gérer des identifiants de connexion pour les divers utilisateurs et aussi de gérer les préférences de ces derniers à l'égard du système.

- Chaque utilisateur devrait pouvoir modifier son profil et ses préférences.
- Les aspects du profil d'utilisation qui ont à voir avec les privilèges d'accès devraient uniquement pouvoir être modifiés par l'utilisateur ayant des privilèges appropriés (comme un utilisateur intensif ou un administrateur du système).

3.2.13. Portail

Le portail vise à donner la possibilité aux FS d'établir un nouveau profil et de présenter de la documentation de mise à jour de profil (mise à jour de certificat d'association professionnelle, de certificat d'assurance responsabilité civile, etc.). Le portail facilitera également la communication de données d'aiguillage aux FS et permettra à ceux-ci de gérer les activités relatives aux dossiers (demandes de prolongation) et de présenter leurs factures et leurs formulaires statistiques.

Le portail doit aussi soutenir les sondages en ligne (à noter que les participants aux sondages doivent rester anonymes).

3.2.14. Gestion des communications

La gestion des communications se définit exclusivement comme la gestion des campagnes de communication.

- Communiquer avec les clients, les organismes, etc. pour la diffusion de mises à jour de politiques, de bulletins d'information, de demandes de renseignements, etc., par les diverses méthodes employées.
- Utiliser un système de rappel.
- Assurer le suivi des réponses.

Un système d'information modernisé aidera les SAE à fournir un service de choix à la clientèle et à respecter les plus hautes normes de confidentialité au profit des clients. L'outil modernisé accélérera les recherches des conseillers qui répondent à des besoins immédiats des employés, permettra de recueillir des données supplémentaires pour une prise de décisions éclairées et rendra les employés des SAE plus efficaces dans leur emploi du temps.

3.3 Exigences relatives aux services de mise en œuvre

L'entrepreneur doit fournir les services de mise en œuvre et de transition associés au SGIPAE proposé nécessaires à la conception d'une solution, à la configuration, à l'installation, au déploiement, à l'intégration, à la mise à l'essai, à la formation et à la préparation à l'utilisation en situation réelle. Les services requis comprennent notamment ce qui suit :

1. services pour la prestation de livrables de planification et de conception pour la transition entre les phases des opérations du projet;
2. services pour la mise en place d'une infrastructure technique et l'installation initiale des principaux produits logiciels commerciaux requis pour appuyer la configuration, la personnalisation, l'intégration et les autres efforts requis pour mettre en place la première vague de services du PAE;
3. services requis pour la configuration, la personnalisation, l'intégration et les autres efforts requis pour mettre en place la première vague de services du PAE et obtenir les autorisations nécessaires pour opérer le SGIPAE dans un environnement de production en service;
4. services requis pour l'inscription des intervenants et la migration des données opérationnelles de l'actuel environnement du PAE vers le SGIPAE.

L'entrepreneur doit fournir les services associés au SGIPAE proposé nécessaires à l'utilisation, à l'entretien et au soutien quotidiens du SGIPAE.

L'entrepreneur peut être tenu de fournir, sur demande, des services de base pour appuyer les nouvelles initiatives relatives aux SAE, notamment la planification de projets, la conception de projets, le déploiement de projets, la mise en œuvre de services opérationnels et la mise en œuvre de services d'infrastructures et d'intégration.

L'entrepreneur peut également devoir fournir, sur demande, des services liés à la prestation de services spéciaux du PAE lorsque de tels services sont requis pour, entre autres, réaliser de meilleures analyses, appuyer de nouvelles modalités ou des modalités supplémentaires aux contrats (p. ex. pour faciliter un accès à distance et au moyen d'appareils mobiles), rédiger des rapports spéciaux ou offrir d'autres services de gestion, de planification ou de prestation liés aux SAE.

Les services doivent être fournis par l'entremise d'une série de tâches autorisées par le Canada dans le cadre d'un processus structuré d'autorisation de tâches (AT).

3.4 Exigences en matière d'accessibilité et de convivialité du Web

L'entrepreneur doit respecter les exigences en matière d'accessibilité et de convivialité du Web établies dans les normes et les lignes directrices ci-après.

1) Norme sur l'accessibilité des sites Web : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601 et lignes directrices sur l'accessibilité du contenu Web : (WCAG) 2.0 : http://www.w3.org/TR/WCAG20/
2) Norme sur la facilité d'emploi des sites Web : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=24227
3) Boîte à outils de l'expérience Web : http://www.tbs-sct.gc.ca/ws-nw/wa-aw/wet-boew/index-fra.asp

Loi sur les langues officielles : https://laws.justice.gc.ca/fra/lois/O-3.01/index.html

4. CALENDRIER PRINCIPAL DE PROJET

Le calendrier principal de projet indique les principaux jalons et livrables des résultats opérationnels ainsi que les principales dates cibles associées à la transition de l'actuelle solution des SAE vers le SGIPAE fourni par l'entrepreneur. Ces dates sont fondées sur le plan de mise en œuvre préliminaire du projet fourni en réponse à la demande de soumissions.

Le calendrier principal de projet est utilisé pour coordonner les livrables et les résultats fournis par l'entrepreneur avec les divers systèmes et services fournis par le gouvernement dont dépend le matériel de l'entrepreneur (p. ex. prestation d'une infrastructure du gouvernement du Canada et technologies et logistiques d'accès connexes).

Le calendrier ci-après combine diverses activités de transition (p. ex. planification, mise en œuvre et mise à l'essai) avec les processus d'approbation et d'acceptation de Santé Canada et la logistique associée à la migration des programmes et des services existants d'aide aux employés vers le nouveau SGIPAE.

Le calendrier commence à la date de début de la planification, qui est au plus tard en octobre 2020, jusqu'à la date de « déploiement » de la couverture de transition en juin 2021.

Tableau 4.1-1 : Résumé du calendrier principal de projet

Jalons clés	Titre	Délai (en mois)	Sommaire des résultats, des livrables et des activités clés
MM-1-CON-0000	Début – début du projet et des phases de planification et de conception	octobre 2020	Début du projet (début du projet, phases de planification et de conception en fonction des livrables de planification définis - AT#1)
MM-1-CON-0100	Phase 1 – Fin des phases de planification et de conception	Début + 1M	Livrables de planification et de conception détaillés en fonction des révisions apportées aux documents par l'entrepreneur après le début du projet et pendant la phase 1 de planification du projet
MM-2-CON-0300	Phase 2 – Fin de la mise en œuvre et du premier déploiement	Début + 5M	Phase 2 – installation du SGIPAE sur les plateformes du GC, configuration pour la première vague de processus opérationnels des SAE et intégration avec les systèmes et services du GC et obtention des approbations requises pour l'utilisation (OA)
MM-3-CON-0500	Phase 3 – Fin des essais d'acceptation des utilisateurs (EAU) et début de la phase 4 de démarcation	Début + 6M	Phase 3 – vague 1 du transfert des SAE en vue des derniers essais d'acceptation de la phase 4 avant la démarcation en vue de la production en direct
MM-4-CON-0100	Fin de la phase 4 de démarcation	Début + 9M (juin 2021)	Phase 4 – démarcation et lancement en direct de la vague 1 du projet de SAE en fonction de l'acceptation par le Canada (y compris les facteurs de sécurité, de performance et d'autres facteurs connexes)
MM-5-CON-	Début de la phase 5 de stabilisation	Début + 9M	Surveillance de la solution en production pour cerner et classer en ordre de priorité les secteurs où des modifications doivent être apportées afin de fournir des services de la vague 1 aux niveaux de service requis, ce qui peut notamment comprendre les services de l'entrepreneur et l'infrastructure et les services du GC.
MM-5-CON-	Fin de la phase 5 de stabilisation	Début + 21M	Finalisation des services, des niveaux de services et des ressources et de l'infrastructure habilitantes requis pour fournir des SAE stables qui cadrent avec les services et les niveaux de services actuels. Évaluation et restructuration des modèles de dotation pour améliorer l'optimisation des ressources du Canada.

APPENDICE A DE L'ANNEXE B – SERVICES D'INFRASTRUCTURE FOURNIS PAR LE GOUVERNEMENT DU CANADA

Le présent appendice décrit la portée des services d'infrastructure de TI qui peuvent être fournis par le Canada en vue du déploiement du SGIPAE. Ces services refléteront notamment les services d'hébergement de SPC et les fournisseurs de services d'infonuagique approuvés ou négociés par SPC qui peuvent être disponibles et qui respectent les exigences en matière de sécurité pour une solution hébergée en nuage.

L'objectif est d'assurer une protection adéquate des données du gouvernement du Canada pour les solutions hébergées en nuage.

1. NORMES DE SERVICE DES CENTRES DE DONNÉES D'ENTREPRISE DE SPC

Disponibilité

- 24 x 7 x 365, 99,982 % du temps

Heures de service

- 24 x 7 x 365 – Sur place

Maintenance régulière planifiée

- Les centres de données d'entreprise sont conçus de sorte qu'aucune activité de maintenance planifiée ne requiert l'arrêt complet des centres (Barrie, Borden et Gatineau).

Heures de soutien du fournisseur externe

- 24 x 7 x 365 – Sur place

Temps moyen de rétablissement

- 1 heure, 90 % du temps

Durée de traitement des demandes

Offre de services	Délai moyen d'exécution	Pourcentage du temps
Consultation sur la planification des installations	• Attestation fondée sur les temps de traitement publiés pour l'intégration opérationnelle d'entreprise de SPC • Planification de la capacité – 15 jours une fois que l'information requise est fournie	80 %

Offre de services	Délai moyen d'exécution	Pourcentage du temps
Accès à l'installation des centres de données	• Jusqu'à cinq jours pour une visite prévue • Une heure pour répondre aux incidents **Exception :** Certaines installations de centres de données régionaux n'ont pas accès à un DCFMS local et par conséquent, d'autres dispositions seront prises.	90 %
Commandes à distance (soutien des périphériques de TI sur place dans l'installation)	Jusqu'à cinq jours pour une visite prévue Une heure pour répondre aux incidents **Exception :** Certaines installations de centres de données régionaux n'ont pas accès à un DCFMS local et par conséquent, d'autres dispositions seront prises.	90 %

Offre de services	Délai moyen d'exécution	Pourcentage du temps
Installation du matériel de TI (planification et installation)	Participation aux réunions de planification avec préavis de 5 jours • Installer les appareils de TI – de 5 à 10 jours selon la complexité et le volume • Câblage des dispositifs – de 5 à 10 jours selon la complexité et le volume • Câblage de base – mesure d'approvisionnement requise, jusqu'à 60 jours pour la livraison et l'installation • Expédition et réception – au moins deux jours ouvrables et doit être planifié pendant les heures d'exploitation de la plateforme de chargement **Exception :** Certaines installations de centres de données régionaux n'ont pas accès à un DCFMS local et par conséquent, d'autres dispositions seront prises.	80 %
Mise hors service du matériel de TI (planification et installation)	• Participation aux réunions de planification avec préavis de 5 jours • Retrait des appareils de TI – au moins 30 jours suivant la demande **Exception :** Certaines installations de centres de données régionaux n'ont pas accès à un DCFMS local et par conséquent, d'autres dispositions seront prises.	90 %

Soutien

Après la première installation – Soutien continu

Les installations de SPC offre des services de soutien en tout temps (là où disponible, voir les heures de service) qui sont offerts par l'entremise du Bureau de service d'entreprise de SPC (habituellement dans le cadre de la réponse à un incident)

Offre de services	Délai moyen d'exécution	Pourcentage du temps
Consultation sur la planification des installations	• Attestation fondée sur les temps de traitement publiés pour l'intégration opérationnelle d'entreprise de SPC • Planification de la capacité – 15 jours une fois que l'information requise est fournie	80 %
Accès à l'installation des centres de données	• Jusqu'à cinq jours pour une visite prévue • Une heure pour répondre aux incidents **Exception :** Certaines installations de centres de données régionaux n'ont pas accès à un DCFMS local et par conséquent, d'autres dispositions seront prises.	90 %
Commandes à distance (soutien des périphériques de TI sur place dans l'installation)	Jusqu'à cinq jours pour une visite prévue Une heure pour répondre aux incidents **Exception :** Certaines installations de centres de données régionaux n'ont pas accès à un DCFMS local et par conséquent, d'autres dispositions seront prises.	90 %

Offre de services	Délai moyen d'exécution	Pourcentage du temps
Installation du matériel de TI (planification et installation)	Participation aux réunions de planification avec préavis de 5 jours • Installer les appareils de TI – de 5 à 10 jours selon la complexité et le volume • Câblage des dispositifs – de 5 à 10 jours selon la complexité et le volume • Câblage de base – mesure d'approvisionnement requise, jusqu'à 60 jours pour la livraison et l'installation • Expédition et réception – au moins deux jours ouvrables et doit être planifié pendant les heures d'exploitation de la plateforme de chargement **Exception :** Certaines installations de centres de données régionaux n'ont pas accès à un DCFMS local et par conséquent, d'autres dispositions seront prises.	80 %
Mise hors service du matériel de TI (planification et installation)	• Participation aux réunions de planification avec préavis de 5 jours • Retrait des appareils de TI – au moins 30 jours suivant la demande **Exception :** Certaines installations de centres de données régionaux n'ont pas accès à un DCFMS local et par conséquent, d'autres dispositions seront prises.	90 %

Modalités

- La prochaine priorité consiste à installer de nouvelles charges de travail en TI dans le nuage public, puis dans les installations des centres de données d'entreprise.
- La migration des charges de travail vers les installations des centres de données d'entreprise est l'option privilégiée pour gérer la croissance et l'obsolescence. La croissance de la TI dans les installations des centres de données existants peut être appuyée s'il s'agit de la seule option technique disponible ET que du financement des clients est disponible ET que la demande cadre avec les lignes directrices sur l'intégrité du programme ET que la capacité actuelle de l'installation est suffisante pour répondre à la demande.
- Dans le cas du renouvellement du bail, les modalités du renouvellement doivent être convenues pour une période d'un an et revues chaque année.

2. NORMES DE SERVICE DE LA BASE DE DONNÉES

- Les services de BD cadrent avec les normes de services des centres de données d'entreprise de SPC.

Normes de service	**Cible**
Disponibilité	Cible de 99,5 % (n'inclus pas la maintenance de routine planifiée)
Heures de service	24 x 7 x 365
Maintenance de routine planifiée	Fenêtre de maintenance de routine mensuelle (4 heures), qui cadre avec la fenêtre de maintenance de routine des centres de données d'entreprise de SPC
Heures de soutien du fournisseur externe	24 x 7 x 365
Temps moyen de restauration	4 heures, présumant qu'une infrastructure sous-jacente est disponible et accessible

<table>
<tr><th>Normes de service</th><th>Cible</th></tr>
<tr><td>Délai de réalisation des demandes</td><td>Variable fondée sur le niveau de complexité, la quantité, les ressources et d’autres facteurs applicables à chaque demande individuelle, mais présumant que des ressources sous-jacentes sont disponibles et accessibles. Exemple de délais pour des demandes simples typiques :
<table>
<tr><th>Demande de service</th><th>Délai de traitement</th></tr>
<tr><td>Installation et configuration d’une base de données</td><td>1 jour ouvrable</td></tr>
<tr><td>Modification des paramètres de la configuration actuelle de la base de données</td><td>1 jour ouvrable</td></tr>
<tr><td>Modification des paramètres existants du matériel de la base de données (p. ex. augmentation des capacités de stockage ou du processeur virtuel)</td><td>1 jour ouvrable</td></tr>
</table></td></tr>
</table>

3. NORMES DE SERVICE DES INTERGICIELS

Disponibilité : 24 x 7 x 365, 95 % du temps

- **Heures de service :** 24 x 7 x 365 heures, à négocier selon l’environnement par l’entremise d’une entente officielle de niveau de service
  - **Disponibilité de la norme :** 95 %, à l’exception des correctifs et de la maintenance prévue
- **Maintenance de routine planifiée :** Une fenêtre d’entretien mensuel obligatoire est négociée en fonction de l’environnement par l’entremise d’une entente de niveau de service.
- **Heures de soutien du fournisseur externe :** Ne s’applique pas. SPC offre à ses partenaires du soutien et communique avec les fournisseurs, au besoin.

Temps moyen de rétablissement du service

- Dépend de la complexité du système et de l’entente de niveau de service

Délai de traitement des demandes

- Variable selon le niveau de complexité, la quantité, les délais, les ressources et d’autres facteurs applicables à chaque demande.

ANNEXE C

CRITÈRES D'ÉVALUATION ET DE QUALIFICATION

1.0 Instructions aux répondants

1.1 Les répondants doivent soumettre leurs réponses conformément aux exigences énoncées à cette annexe.

1.2 Dans sa réponse, le répondant doit démontrer qu'il comprend les exigences contenues dans l'IQ et expliquer comment il y répondra. Le répondant doit démontrer son expérience et décrire de manière exhaustive, concise et claire l'approche qu'il adoptera pour exécuter le projet.

1.3 La réponse doit traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères obligatoires et cotés en fonction desquels la réponse sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans l'IQ.

1.4 Si le nombre de projets présentés en référence dans la réponse dépasse la limite établie dans les exigences relatives au contenu de la réponse, les projets seront évalués selon l'ordre dans lequel ils sont fournis et les projets dépassant le nombre demandé ne seront pas évalués.

1.5 Un même projet peut servir à l'égard de plus d'une exigence. Cependant, le répondant doit remplir un formulaire d'expérience relative au projet pour chaque projet cité en référence (même si ce projet est cité plus d'une fois) et ne devrait pas renvoyer à des projets dont il est question ailleurs dans sa réponse. Par exemple, si le répondant parle d'un projet en C-1 et qu'il entend utiliser le même projet en C-2, il doit remplir un formulaire distinct pour C-1 et C-2.

2.0 Sommaire et méthode de l'évaluation de l'IQ

2.1 L'IQ comportera un processus d'évaluation en deux étapes : a) un ensemble de critères généraux obligatoires (11 éléments) établissant les exigences fondamentales du fournisseur pour cette activité, et b) un ensemble de mesures cotées (critères d'évaluation cotés) découlant des critères obligatoires. Les critères obligatoires visent à s'assurer qu'un fournisseur éventuel est en mesure de répondre à l'exigence générale de fournir un SGIPAE commercial disponible sur le marché. Ensuite, les mesures cotées servent à obtenir un classement objectif des organisations qui répondent à toutes les exigences obligatoires afin d'établir une liste de huit organisations qui sont objectivement les mieux placées pour répondre aux besoins fondamentaux de Santé Canada.

2.2 Les critères obligatoires seront évalués selon le principe de réussite ou d'échec (c'est-à-dire recevable/non recevable) indiqués à la section 3.1 – Critères techniques obligatoires. Pour que leur réponse soit recevable, les répondants doivent clairement préciser comment ils répondent aux critères établis dans l'exigence obligatoire. Il ne suffit pas de déclarer simplement que le répondant se conforme à l'exigence. La réponse ne satisfera pas à un critère obligatoire admissible si le Canada détermine que les

renseignements fournis ne décrivent pas suffisamment en détail de quelle façon le répondant satisfait à une ou à plusieurs exigences obligatoires.

2.3 Les réponses aux critères d'évaluation cotés seront évaluées conformément aux pondérations applicables figurant à l'appendice A – Pondérations applicables aux critères d'évaluation cotés.

2.4 Les réponses seront évaluées conformément aux critères et aux facteurs de pondération indiqués à la section 3.2 Critères technique cotés et à l'appendice A de l'annexe C. Ces critères ne sont pas évalués selon le principe de réussite ou d'échec.

2.5 Chaque projet cité en référence en lien avec l'expérience évaluée selon les critères C-x, C-y, sera coté séparément en fonction des critères d'évaluation cotés. Une moyenne des notes individuelles sera alors effectuée pour obtenir une note globale, puis la pondération applicable sera appliquée.

2.6 Une fois l'évaluation terminée pour toutes les propositions des fournisseurs, les huit fournisseurs ayant obtenu les meilleures notes seront invités à participer au processus d'approvisionnement.

3.0 Évaluation technique

3.1 Critères techniques obligatoires

Les critères obligatoires énumérés ci-dessous seront évalués selon le principe « satisfait/non satisfait » (c'est-à-dire recevable/non recevable ou conforme/non conforme).

Lorsqu'un critère obligatoire invite un répondant à **« démontrer »**, pour être recevable, la réponse technique doit décrire de quelle manière le répondant répond aux critères établis dans l'exigence obligatoire. La justification ne doit pas être une simple répétition des exigences, mais doit fournir suffisamment de détails pour démontrer la façon dont le répondant satisfera aux exigences. Il ne suffit pas de simplement déclarer que la réponse est conforme à l'exigence. La réponse ne satisfera pas à un critère obligatoire si le Canada détermine que la justification ne décrit pas suffisamment en détail la manière dont le répondant démontre sa conformité à une ou à plusieurs exigences obligatoires.

Nº	Critères obligatoires	Satisfait (Oui/Non)	Numéro(s) de page dans la réponse
O-1	**SGIPAE proposé** Le répondant doit décrire le SGIPAE de base proposé qui constituerait la base d'une solution de Services d'aide aux employés de Santé Canada (SAE-SC). Plus précisément, le répondant doit clairement décrire la structure globale du SGIPAE proposé, notamment ce qui suit :		

Nº	Critères obligatoires	Satisfait (Oui/Non)	Numéro(s) de page dans la réponse
	1. Produits, modules, composants ou autres logiciels sous licence proposés pour répondre aux exigences fonctionnelles du SGIPAE définies à l'annexe B – Énoncé des besoins. 2. Dépendances à l'égard de tout logiciel commercial sous-jacent, y compris, sans toutefois s'y limiter, base de données, système d'exploitation, programmes de gestion de la sécurité ou des accès.		
	Réponse		
O-2	**<u>SGIPAE proposé</u>** Pour **chacun** des produits, modules, composants ou autres logiciels sous licence proposés pour répondre aux exigences fonctionnelles du SGIPAE définies à l'annexe B – Énoncé des besoins, le répondant doit fournir les données suivantes : 1. Le nom commercial sous lequel le SGIPAE proposé est vendu. 2. La version du SGIPAE proposé. 3. Le mois et l'année où la version initiale du SGIPAE proposé a été lancée. 4. L'entité qui détient les droits de propriété intellectuelle du SGIPAE proposé. **Note :** Lorsque le SGIPAE proposé est constitué de plusieurs produits visant à offrir une solution intégrée permettant de satisfaire à cette exigence de SC, les points 1 à 4 doivent être traités pour chacun de ces produits.		
	Réponse		
O-3	**<u>Solution proposée – Disponibilité commerciale</u>** Le SGIPAE de base qui est proposé doit être offert sur le marché. Les répondants doivent démontrer sa conformité en fournissant des documents indiquant que le SGIPAE de base est disponible sur le marché. Aux fins de la présente IQ, « offert sur le marché » signifie que le logiciel ou les services proposés doivent pouvoir être achetés librement, qu'ils sont assortis d'une définition de produit/services et d'une structure de prix, et qu'ils font l'objet d'un financement continu en matière de développement et de		

Nº	Critères obligatoires	Satisfait (Oui/Non)	Numéro(s) de page dans la réponse
	soutien. Dans le cas où la solution consiste en plusieurs produits indépendants, chaque produit proposé doit être « offert sur le marché » conformément à la définition ci-dessus. **Les versions ALPHA ou BETA d'un produit ou d'un service ne sont PAS considérées comme étant offertes sur le marché.**		
	Réponse		
O-4	**Structure proposée par le répondant** Le répondant doit décrire la structure du **projet** de SGIPAE proposé en fournissant des détails sur : 1. Le répondant et toute société affiliée employée dans la mise en œuvre du SGIPAE proposé. 2. Tous les fournisseurs des composants du SGIPAE de base nécessaires à la mise en œuvre du SGIPAE proposé. 3. Tous les fournisseurs de services professionnels proposés par le répondant pour fournir et mettre en œuvre le SGIPAE proposé (p. ex. les sous-traitants engagés par le répondant aux fins de la configuration, de l'intégration et de la personnalisation de la solution ou de la prestation de services de soutien).		
	Réponse		
O-5	**Structure proposée par le répondant** Le répondant doit démontrer qu'il est autorisé à fournir et à mettre en œuvre le SGIPAE proposé en fournissant ce qui suit : 1. Si le répondant est l'éditeur de tout élément des produits logiciels privés proposés, le Canada exige que le soumissionnaire confirme, par écrit, qu'il est l'éditeur de logiciel. On demande aux répondants d'utiliser le formulaire d'attestation de l'éditeur de logiciel joint à la présente IQ. Bien qu'il soit nécessaire de fournir tous les renseignements demandés dans le formulaire d'attestation de l'éditeur de logiciel, l'utilisation de ce formulaire n'est pas obligatoire. Pour les répondants qui utilisent un autre formulaire, le Canada déterminera, à sa seule discrétion, si tous les renseignements exigés ont été fournis. Toute modification aux énoncés du formulaire pourrait rendre la réponse non recevable. ou		

Nº	Critères obligatoires	Satisfait (Oui/Non)	Numéro(s) de page dans la réponse
	2. Tout répondant qui n'est pas l'éditeur de tous les produits logiciels proposés dans le cadre de sa réponse doit présenter une preuve de l'autorisation de l'éditeur de logiciel, qui doit être signée par ce dernier (et non par le répondant). Aucune suite ne sera accordée à un répondant qui n'est pas l'éditeur de tous les logiciels privés proposés au Canada, à moins qu'une preuve de l'autorisation de ce dernier n'ait été fournie au Canada. Si les logiciels privés proposés par le répondant proviennent de plusieurs éditeurs de logiciel, une autorisation est exigée de chaque éditeur de logiciel. On demande aux répondants d'utiliser le formulaire d'autorisation de l'éditeur de logiciel joint à la présente IQ. Bien qu'il soit nécessaire de fournir tous les renseignements demandés dans le formulaire d'autorisation de l'éditeur de logiciel, l'utilisation de ce formulaire n'est pas obligatoire. Pour les répondants qui utilisent un autre formulaire, le Canada déterminera, à sa seule discrétion, si tous les renseignements exigés ont été fournis. Toute modification aux énoncés du formulaire pourrait rendre la réponse non recevable. **Notes :** 1. Dans le cadre de la présente IQ, « éditeur de logiciels » désigne le propriétaire de tout produit logiciel compris dans la réponse qui a le droit d'octroyer une licence (et d'autoriser d'autres personnes à octroyer une licence ou une sous-licence) pour ses produits logiciels. 2. Lorsque le logiciel du SGIPAE de base proposé est constitué de plusieurs produits visant à offrir une solution intégrée permettant de satisfaire à cette exigence de SC, le répondant doit être autorisé à fournir chacun de ces produits en présentant les attestations requises pour chaque produit.		
	Réponse		
O-6	**<u>Solution proposée – Sécurité</u>** Le SGIPAE de base proposé doit pouvoir être déployé dans un environnement opérationnel sécurisé qui répond aux exigences du gouvernement du Canada en matière de sécurité. Les répondants doivent démontrer leur conformité en attestant que le SGIPAE de base proposé est : 1. Prêt à être déployé : a. sur une plateforme d'exploitation sécurisée fournie par le Canada (p. ex. par des services de plateforme informatique et d'entreposage fournis à l'interne ou par un		

Nº	Critères obligatoires	Satisfait (Oui/Non)	Numéro(s) de page dans la réponse
	fournisseur tiers de services de plateforme sécurisée sanctionné par le GC); OU, b. comme une offre de bout en bout, clé en main (également appelée « logiciel-service ») fournie par un fournisseur tiers de services de plateforme sécurisée sanctionné par le GC. 2. Prêt à être déployé dans une installation informatique approuvée par le GC située à l'intérieur des frontières géographiques du Canada. Notes: • La liste des fournisseurs tiers de services de plateforme sécurisée sanctionnés par le GC est disponible à cette adresse web : https://cloud-broker.canada.ca/s/?language=fr • Le Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100) est disponible à cette adresse web : https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux.		
	Réponse		
O-7	**Références pour le déploiement du SGIPAE** Le répondant doit fournir deux (2) exemples de projets pertinents en remplissant le formulaire de références pour le déploiement de solutions logicielles (formulaire C-1, fourni à l'appendice A de l'annexe C) pour chaque exemple de projet. Chaque référence pour le déploiement de solutions logicielles fournie doit concerner le déploiement du SGIPAE de base proposé ou d'une version antérieure du SGIPAE de base proposé pour un client externe. Chaque référence pour le déploiement de solutions logicielles fournie doit avoir été en production pendant une période d'au moins 12 mois à compter du déploiement initial. **Note :** Les références pour le déploiement de solutions logicielles fournies seront cotées comme il est stipulé dans le formulaire C-1.		
	Réponse		

Nº	Critères obligatoires	Satisfait (Oui/Non)	Numéro(s) de page dans la réponse
O-8	**Structure proposée par le répondant – Rôles et responsabilités** Le répondant doit décrire les rôles et les responsabilités de chaque entité définie dans la réponse au critère O-4 ci-dessus. Le répondant doit clairement définir : 1. L'entité/les entités ayant des rôles et des responsabilités liés à la fourniture des composants du SGIPAE de base requis pour la fourniture du SGIPAE proposé – p. ex. l'entité qui est l'éditeur de logiciels ou le titulaire de la licence du composant de la solution logicielle proposée. 2. L'entité/les entités responsable(s) de la maintenance de tout logiciel sous licence en tant qu'éditeur de logiciels ou titulaire de la licence du composant de la solution logicielle proposée. 3. L'entité/les entités responsable(s) de la conception, de la configuration, du déploiement et du soutien continu du SGIPAE proposé comme il a été déployé en production réelle pour répondre aux besoins de ce SGIPAE.		
	Réponse		
O-9	**Références des fournisseurs du SGIPAE** Le répondant doit fournir deux (2) exemples de projets pertinents en remplissant le formulaire de références pour les services liés au projet de mise en œuvre du SGIPAE (joint en annexe C-2) pour chaque exemple de projet. Chaque référence de services liés au projet de mise en œuvre du SGIPAE doit concerner le déploiement du SGIPAE de base proposé ou d'une version précédente du SGIPAE de base proposé. Chaque référence de services liés au projet de mise en œuvre du SGIPAE doit comprendre la prestation de services par l'organisation répondante et inclure des services pour l'installation, la configuration, l'intégration, le déploiement, la transition vers l'utilisation réelle et le soutien continu conforme à l'exécution du SGIPAE. **Note :** Les références des services liés au projet de mise en œuvre du SGIPAE fournies seront cotées comme il est stipulé dans le formulaire C-2.		
	Réponse		

Nº	Critères obligatoires	Satisfait (Oui/Non)	Numéro(s) de page dans la réponse
O-10	**Profil du répondant – Viabilité financière** Le répondant doit être financièrement viable pour répondre à ce besoin. En soumettant une proposition dans le cadre de la présente IQ, tout répondant aura consenti à ce que le Canada effectue sa propre évaluation de la viabilité financière du répondant. Pour déterminer la viabilité financière du répondant, le Canada exigera, en envoyant un avis écrit au répondant, que ce dernier fournisse des renseignements financiers décrits dans le corps du texte de la section 4.4 de l'IQ : Évaluation de la viabilité financière. Les répondants doivent indiquer dans la réponse ci-dessous qu'ils reconnaissent et acceptent que le Canada effectue sa propre évaluation de la viabilité financière du répondant. Les répondants qui ne donnent pas ce consentement ou dont la viabilité financière est jugée insuffisante par le Canada seront retirés du processus de sélection.		
	Réponse **Réponse – accepter les dispositions**		
O-11	**Solution proposée – Interface et prise en charge bilingues** La solution doit prendre en charge les deux langues officielles du Canada (français et anglais). Les répondants doivent démontrer leur conformité en fournissant des exemples de documents en français et en anglais qui illustrent la prise en charge multilingue du produit. Les exemples de documents à l'appui comprennent, sans s'y limiter, des captures d'écran de sessions d'utilisateurs dans les deux langues officielles (p. ex. capture d'écran de la session en anglais, capture d'écran de la session en français), de la documentation pour les utilisateurs, du matériel de formation ou d'autres documents démontrant l'utilisation du produit dans les deux langues. Si la solution n'est pas bilingue comme décrit ci-dessus, le répondant doit fournir une feuille de route détaillée indiquant les délais requis par le répondant pour produire et fournir une solution entièrement bilingue.		
	Réponse		

3.2 Critères techniques cotés

Les réponses seront évaluées en fonction des critères techniques cotés suivants, en utilisant les facteurs d'évaluation et les indicateurs de pondération précisés pour chaque critère. Les réponses qui ne satisfont pas aux notes pondérées minimales indiquées seront jugées comme non recevables.

#	Critères d'évaluation cotés	Méthode de notation
C-1	**Capacité organisationnelle du répondant**	
C-1.1	**<u>Compréhension des exigences du projet de SAE</u>** Le répondant devrait démontrer qu'il comprend les exigences et les produits livrables du projet de SAE de Santé Canada conformément à ce qui est décrit à l'annexe B – Énoncé des besoins, en décrivant de façon concise et dans ses propres mots : 1. Les objectifs généraux du projet conformément à ce qui est décrit à l'annexe B – Énoncé des besoins. 2. L'environnement cible du SGIPAE comme le prévoit le Canada. 3. L'approche globale de mise en œuvre progressive et le calendrier du projet. 4. Le rôle du Canada dans la fourniture d'infrastructures et de services à l'appui de l'environnement cible. 5. La portée du SGIPAE requis pour soutenir les projets de déploiement de la première vague. 6. La portée possible des services en réponse aux changements de technologie, de politique et d'exigences commerciales au cours du cycle de vie du projet. 7. Les exigences de réduction des risques dans l'approche de migration et de déploiement adoptée. 8. Les exigences de sécurité associées au projet.	Les points seront attribués de la manière suivante : **5 pts** = la réponse traite 7 ou plus points 1 à 8 **4 pts** = la réponse traite 5 ou 6 des points 1 à 8 **3 pts** = la réponse traite 4 des points 1 à 8 **2 pts** = la réponse traite 3 des points 1 à 8 **1 pt** = la réponse traite 2 des points 1 à 8 **0 pt** = la réponse traite moins de 2 des points 1 à 8 **Note :** L'expression « traite un point » signifie que le répondant a fourni suffisamment de détails pour démontrer le point en question (p. ex. reconnaissance de l'exigence d'utiliser les systèmes et services de gestion des appels et de base de connaissances fournis par le gouvernement) et qu'il reconnaît qu'il s'agit d'une exigence qui doit être abordée dans le cadre du projet et a formulé ses hypothèses dans le contenu de sa réponse. **Les réponses à ce critère qui contiennent une quantité excessive de texte copié directement de l'IQ et/ou de documents à l'appui ne seront pas considérées comme indiquant une compréhension des exigences et des produits livrables du projet de SAE proposé par Santé Canada.**
Réponse :		
C-1.2	**<u>Maturité organisationnelle du répondant – Années</u>** Le répondant devrait indiquer le nombre d'années depuis lesquelles il fournit un SGIPAE (comme il est défini à l'annexe B – Énoncé des	Les points seront attribués de la manière suivante : **5 pts** = 7 ans ou plus de mise en œuvre d'un SGIPAE au Canada **4 pts** = ≥ 5 à < 7 ans **3 pts** = ≥ 4 à < 5 ans

#	Critères d'évaluation cotés	Méthode de notation
	besoins) au Canada.	**2 pts** = ≥ 3 à < 4 ans **1 pt** = ≥ 2 à < 3 ans **0 pt** = < 2 ans ou aucune réponse comparable
Réponse :		
C-1.3	**Profil du répondant – Organisation de prestation de services du SGIPAE de base** Le répondant devrait disposer d'une unité opérationnelle existante qui se concentre sur la prestation de services professionnels à l'appui de la conception, de la configuration, du déploiement et du soutien continu du SGIPAE (comme il est défini à l'annexe B – Énoncé des besoins) pour les clients externes (c'est-à-dire les organisations tierces non affiliées au répondant). Le répondant devrait démontrer sa conformité en décrivant : 1. L'unité opérationnelle du SGIPAE explicitement chargée de la mise en œuvre du SGIPAE et des solutions. 2. Où se trouve l'unité opérationnelle du SGIPAE dans la structure organisationnelle du répondant (p. ex. en fournissant une structure organisationnelle qui indique clairement la place qu'occupe l'unité opérationnelle du SGIPAE).	Les points seront attribués de la manière suivante : **5 pts =** lorsque le répondant mentionne une unité opérationnelle précise explicitement chargée de la mise en œuvre du SGIPAE, comme il est défini à l'annexe B – Énoncé des besoins, où la prestation des services connexes du SGIPAE constitue l'activité principale de l'organisation, et qu'il décrit la place qu'occupe l'unité opérationnelle du SGIPAE dans la structure organisationnelle du répondant. **4 pts** = lorsque le répondant mentionne une unité opérationnelle précise dont la responsabilité principale est la mise en œuvre du SGIPAE, comme il est défini à l'annexe B – Énoncé des besoins, mais que la prestation des services connexes du SGIPAE **ne** constitue **pas** l'activité principale de l'organisation citée (c'est-à-dire qu'elle fait partie d'un portefeuille de secteurs d'activité pris en charge par l'organisation), et qu'il décrit la place qu'occupe l'unité opérationnelle du SGIPAE dans la structure organisationnelle du répondant **3 pts** = lorsque le répondant dispose d'une unité opérationnelle dotée de ressources chargées de fournir un SGIPAE à des organisations clientes en fonction de la demande et des besoins. **0 pt =** lorsque le répondant ne démontre aucune capacité en matière de SGIPAE.
Réponse :		
C-1.4	**Profil du répondant – Portefeuille de services du fournisseur du SGIPAE de base**	Les points seront attribués de la manière suivante : **5 pts** = lorsque le répondant décrit les services fournis par l'unité

#	Critères d'évaluation cotés	Méthode de notation
	Le répondant devrait démontrer le portefeuille du SGIPAE fourni par l'unité opérationnelle en énumérant les services fournis. Les services doivent comprendre, sans toutefois s'y limiter, les éléments suivants : 1. Services de soutien à la transition d'entrée, qui comprennent entre autres la conception de solutions, la configuration, l'installation, le déploiement, l'intégration, la mise à l'essai, la formation et la préparation à la production réelle. 2. Services de soutien aux activités courantes, qui comprennent entre autres le fonctionnement, l'entretien et le soutien continus du SGIPAE déployé.	opérationnelle qui comprennent tous les services énumérés aux points 1 et 2, lesquels sont des activités essentielles de l'organisation indiquée, et démontre de manière exhaustive que les services essentiels sont conformes au SGIPAE déployé. **4 pts**= lorsque le répondant décrit les services fournis par l'unité opérationnelle qui comprennent tous les services énumérés aux points 1 et 2, lesquels sont des activités essentielles de l'organisation indiquée, et démontre de manière significative que les services essentiels sont conformes au SGIPAE déployé, **3 pts** = lorsque le répondant décrit les services fournis par l'unité opérationnelle qui comprennent tous les services énumérés aux points 1 et 2, lesquels sont des activités essentielles de l'organisation indiquée, et démontre de manière adéquate que les services essentiels sont conformes au SGIPAE déployé. **2 pts** = lorsque le répondant décrit les services fournis par l'unité opérationnelle qui comprennent tous les services énumérés aux points 1 et 2, et que les services liés au SGIPAE ne sont pas des activités essentielles de l'organisation indiquée, et démontre avec un minimum de détails que les services essentiels sont conformes au SGIPAE déployé. **0 Pt =** lorsque le répondant n'a pas suffisamment démontré un degré adéquat de compréhension de l'exigence ou lorsque le répondant n'a pas fourni de réponse pertinente.
Réponse :		
C-1.5	**<u>Maturité organisationnelle du répondant – Projets de déploiement du fournisseur du SGIPAE</u>** Le répondant devrait indiquer le nombre de projets de déploiement actif pour lesquels le fournisseur du SGIPAE proposé a déployé le SGIPAE de base proposé en production réelle. **Note :** un projet de déploiement actif est un déploiement du SGIPAE de base proposé, ou d'une version antérieure, qui est utilisé en production réelle par une organisation cliente afin de fournir des SAE.	Les points seront attribués de la manière suivante : **5 pts** = 5 projets de déploiement ou plus **4 pts** = 4 projets de déploiement **3 pts** = 3 projets de déploiement **2 pts** = 2 projets de déploiement **1 pt** = 1 projet de déploiement **0 pt** = aucun projet de déploiement

#	Critères d'évaluation cotés	Méthode de notation
Réponse :		
C-2	**Solution proposée**	
C-2.1	**<u>Solution proposée – Fonctionnalité de la solution de base</u>** Le répondant devait décrire le SGIPAE de base proposé qui constituerait le fondement d'une solution en matière de SAE-SC. Plus précisément, le répondant devrait décrire les composants de la solution logicielle de base qui, globalement, fourniront la solution telle qu'elle sera déployée et qui incluront ce qui suit : 1. Gestion des nouveaux dossiers comme il est défini dans l'annexe B, section 3.2.1. 2. Gestion des cas comme il est défini dans l'annexe B, section 3.2.2. 3. Assurance qualité comme il est défini dans l'annexe B, section 3.2.3. 4. Gestion des prestataires de services comme il est défini dans l'annexe B, section 3.2.4. 5. Gestion des aiguillages comme il est défini dans l'annexe B, section 3.2.5. 6. Gestion des comptes de l'organisation comme il est défini dans l'annexe B, section 3.2.6. 7. Administration financière comme il est défini dans l'annexe B, section 3.2.9. 8. Gestion des rapports comme il est défini dans l'annexe B, section 3.2.11. 9. Gestion des utilisateurs comme il est défini dans l'annexe B, section 3.2.12. 10. Services du portail comme il est défini dans l'annexe B, section 3.2.13. 11. Gestion de la communication comme il est défini dans l'annexe B, section 3.2.14.	Les points seront attribués de la manière suivante : **5 pts** = la réponse traite 10 ou plus des points 1 à 11 et contient des exemples de documents démontrant comment chaque point est traité. **4 pts** = la réponse traite 8 ou 9 des points 1 à 11 et contient des exemples de documents démontrant comment chaque point est traité. **3 pts** = la réponse traite 7 des points 1 à 11 et contient des exemples de documents démontrant comment chaque point est traité. **2 pts** = la réponse traite 6 des points 1 à 11 et contient des exemples de documents démontrant comment chaque point est traité, **ou** traite plus de 6 points, mais sans exemple de documents démontrant comment chaque point est traité. **1 pt** = la réponse traite 4 ou 5 des points 1 à 11 et contient des exemples de documents démontrant comment chaque point est abordé, **ou** traite plus de 4 points, mais sans exemple de documents démontrant comment chaque point est traité. **0 pt** = la réponse traite moins de 4 des points 1 à 11 ou ne fournit aucune réponse pertinente.

#	Critères d'évaluation cotés	Méthode de notation
Réponse :		
C-2.2	**Solution proposée – Architecture de la solution** Le répondant devrait décrire l'architecture globale du SGIPAE. Le SGIPAE devrait être construit sur une architecture ouverte fondée sur des normes, c'est-à-dire : 1. une architecture Web disponible publiquement et publiée, utilisant des définitions normalisées, notamment celles de J2EE, .net et XML. 2. une architecture dans laquelle chaque élément fonctionnel est mis en œuvre sur des plateformes matérielles distinctes et mis à l'échelle individuellement (p. ex. services d'accès aux utilisateurs, fonctions des services d'application du SGIPAE). 3. une architecture basée sur un système composite pour associer et dissocier des composants de la solution et permettre une utilisation maximale des ressources existantes ainsi qu'une souplesse continue dès le départ. L'utilisation comprendra un processus d'écologisation continue dans le cadre duquel aucun composant modifié, remplacé, mis à niveau ou échangé n'entraînera l'effondrement du système dans son ensemble.	Les points seront attribués de la manière suivante : **5 pts =** lorsque le répondant a répondu aux exigences des **points 1 à 3** en fournissant des détails exhaustifs dans le plan de la solution et a adapté sa réponse au SGIPAE. **4 pts =** lorsque le répondant a répondu aux exigences des **points 1 à 3** en fournissant des détails significatifs dans le plan de la solution et a adapté sa réponse au SGIPAE. **3 pts =** lorsque le répondant a répondu aux exigences des **points 1 à 3** en fournissant des détails adéquats dans le plan de la solution et a adapté sa réponse au SGIPAE. **2 pts =** lorsque le répondant a à peine répondu aux exigences des **points 1 à 3** ou n'a pas adapté sa réponse au SGIPAE. **0 pt =** lorsque le répondant n'a pas suffisamment démontré un degré de compréhension adéquat de l'exigence ou lorsqu'il n'a pas fourni de réponse pertinente.
Réponse :		
C-2.3	**Solution proposée – Options de déploiement** Le répondant devrait énoncer les options de déploiement possibles du SGIPAE de base proposé, lesquelles comprennent les suivantes :	Les points seront attribués de la manière suivante : **5 pts** = Plusieurs options de déploiement, dont 1 et 2 **4 pts** = option de déploiement 1 uniquement **3 pts** = option de déploiement 2 uniquement **0 pt** = Pas d'option de déploiement

#	Critères d'évaluation cotés	Méthode de notation
	1. Déploiement en nuage public[1] 2. Déploiement sur place chez les clients	
Réponse :		
C-3	**Sécurité et accessibilité**	
C-3.1	**<u>Sécurité de projet – Politique de sécurité</u>** Le répondant devrait démontrer qu'il dispose d'une politique de sécurité exhaustive conforme aux exigences de sécurité de cette initiative de SAE de Santé Canada. Le répondant devrait démontrer que la politique de sécurité proposée répond à ces exigences : 1. L'obligation que seules les ressources qui possèdent le niveau d'attestation de sécurité requis pour exécuter une tâche, soient autorisées à accéder à des renseignements ou à des biens protégés, ou à des établissements dont l'accès est réglementé. 2. L'obligation de veiller à ce que la politique de sécurité soit appliquée dans l'ensemble de l'équipe de répondants, notamment tous les sous-traitants. **La politique de sécurité des organisations sous-traitantes ne sera pas acceptée aux fins d'évaluation en réponse à ce critère..**	Les points seront attribués de la manière suivante : **5 pts** = La réponse satisfait aux exigences des points 1 et 2 et est adaptée au projet de SAE de Santé Canada **3 pts** = La réponse satisfait aux exigences des points 1 ou 2 et est a adaptée au projet de SAE de Santé Canada **2 pts** = La réponse satisfait aux exigences de l'un des points 1 ou 2 et n'est **pas** adaptée au projet de SAE de Santé Canada. **0 pt** = La réponse ne traite aucun point.
Réponse :		
C-3.2	**<u>Accessibilité – Règles WCAG 2.1 AA</u>** Le répondant devrait démontrer le niveau de conformité de son SGIPAE de base au critère 2.1 de niveau AA des Règles pour l'accessibilité aux contenus Web (WCAG) du Consortium World Wide	Les points seront attribués de la manière suivante : **5 pts =** La solution est conforme au critère WCAG 2.1 de niveau AA ou de niveau supérieur. **4 pts =** La solution répond au critère WCAG 2.0 de niveau AA ou au

[1] Nuage public : Un produit commercial ayant fait l'objet d'une évaluation de sécurité et acquis pour être utilisé par toutes les organisations gouvernementales. Dans ce modèle de déploiement, les organisations gouvernementales partageront de façon sécuritaire la location avec des entreprises privées, des organismes à but non lucratif et des particuliers.

#	Critères d'évaluation cotés	Méthode de notation
	Web (W3C), comme il est défini dans la norme sur l'accessibilité des sites Web du gouvernement du Canada. **Le soumissionnaire devrait décrire en détail comment l'accessibilité est intégrée à la solution proposée du point de vue de son cycle de mise à jour de la solution.**	critère WCAG 2.1 de niveau A et s'accompagne d'un plan réalisable ou d'un cycle de lancement de produit afin de passer au critère WCAG 2.1 de niveau AA ou de niveau supérieur. **3 pts =** La solution répond partiellement au critère WCAG 2.0 de niveau AA ou de niveau supérieur et s'accompagne d'un plan d'action ou d'un cycle de mise à jour du produit afin passer au critère WCAG 2.0 de niveau AA ou de niveau supérieur. **0 pt =** La solution ne répond pas aux exigences minimales du critère WCAG 2.0 de niveau AA ou il n'y a pas de processus pour effectuer une évaluation.
Réponse :		

Appendice A de l’annexe C : Formulaires de références de projets

Cette annexe aux exigences cotées fournit les modèles pour les références de projets :

1. Formulaire C-1 – Références de déploiement de solutions logicielles précédentes – 2 projets de référence sont requis en réponse au critère obligatoire O-7.
2. Formulaire C-2 – Références des services liés au projet de mise en œuvre du SGIPAE – 2 projets de référence sont requis en réponse au critère obligatoire O-9

Les répondants peuvent utiliser le même projet cité en référence en réponse à chacune de ces exigences. Les répondants doivent s’assurer que les réponses sont complètes et fournir les formulaires de référence requis dûment remplis.

Par souci de clarté, bien qu’un même projet puisse être utilisé dans chaque cas, chaque ensemble de projets de référence doit avoir un objectif précis et des critères différents.

La personne-ressource du client citée en référence dans la section Référence du client doit être en mesure de confirmer sans ambiguïté que le répondant, ou ses sociétés affiliées, ont fourni les services énoncés dans le modèle de référence du client. Pour plus de clarté, si la personne-ressource du client citée en référence est incapable de confirmer sans ambiguïté que le répondant ou ses sociétés affiliées ont fourni les services (p. ex. en invoquant un manque de connaissance ou d’autorité pour fournir une telle confirmation sans ambiguïté, ou en laissant entendre un tel manque de connaissance en contestant la prestation de ces services par le répondant), le Canada interprétera alors cette incapacité à fournir une réponse sans ambiguïté comme une absence de confirmation de la conformité et jugera la proposition non conforme aux exigences.

Il incombe au répondant de s’assurer que la personne-ressource du client citée en référence est en mesure de confirmer sans ambiguïté ou de contester que le répondant, ou ses sociétés affiliées, ont fourni les services décrits dans le modèle de référence du client.

Formulaire C-1 Références de déploiement de solutions logicielles précédentes

Instructions pour remplir le formulaire :

1. Deux (2) exemples de projets pertinents doivent être fournis.
2. Un formulaire distinct de Références de déploiement de solutions logicielles doit être rempli pour chaque exemple de projet.
3. Les réponses seront utilisées pour classer les références fournies en réponse au critère O-7 (Références pour le déploiement du SGIPAE).

Référence 1

Répondant	
Client	
Nom de la personne-ressource	
Titre de la personne-ressource	
Numéro de téléphone	
Nom du projet	
Bref aperçu du projet	
Échéancier du projet	

Références de déploiement de solutions logicielles précédentes – Référence 1				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
1	Le répondant devrait indiquer que SGIPAE de base fourni, déployé et exploité dans le cadre du projet cité en référence fonctionne à l'aide des modules logiciels et aux niveaux d'édition proposés.	25 %	Les points seront attribués de la manière suivante : **5 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels et aux niveaux d'édition proposés. **4 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels proposés à des niveaux d'édition qui ne sont pas à plus d'un niveau d'édition majeur avant le niveau d'édition actuel. **3 pts =** le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels proposés à des niveaux d'édition qui ne sont pas à plus de deux niveaux d'édition majeurs avant le niveau d'édition actuel. **2 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne en utilisant les modules logiciels proposés à des niveaux d'édition qui sont à plus de deux niveaux d'édition majeurs avant le niveau d'édition actuel **0 pt** = le SGIPAE de base fourni et déployé dans le projet cité en référence ne fonctionne pas à l'aide des modules logiciels proposés ou aucune réponse comparable.	
2	Le répondant devrait indiquer la date à laquelle le projet de préférence est entré en production réelle avec le SGIPAE. Par souci de clarté, le SGIPAE est entré en production réelle lorsque les fonctionnalités / modules suivants sont passés au mode de production réelle : 1. Gestion des nouveaux dossiers comme il est défini dans l'annexe B, section 3.2.1. 2. Gestion des cas comme il est défini dans l'annexe B, section 3.2.2.	10 %	Les points seront attribués de la manière suivante : **5 pts** = ≥ 36 mois avant la date de clôture de l'IQ **4 pts** = < 36 mois à ≥ 24 mois avant la date de clôture de l'IQ **3 pts** = < 24 mois à ≥ 12 mois avant la date de clôture de l'IQ **2 pts** = < 12 mois avant la date de clôture de l'IQ **0 pt** = pas en production réelle ou pas de réponse comparable.	

Références de déploiement de solutions logicielles précédentes – Référence 1				
N°	Critères	Pondération	Méthode de notation	Réponse
	3. Assurance qualité comme il est défini dans l'annexe B, section 3.2.3. 4. Gestion des prestataires de services comme il est défini dans l'annexe B, section 3.2.4. 5. Gestion des aiguillages comme il est défini dans l'annexe B, section 3.2.5. 6. Gestion des comptes de l'organisation comme il est défini dans l'annexe B, section 3.2.6. 7. Administration financière comme il est défini dans l'annexe B, section 3.2.11.			
3	Le répondant devrait préciser les langues prises en charge dans le projet cité en référence, les langues en question devant inclure l'anglais et le français.	15 %	Les points seront attribués de la manière suivante : **5 pts** = les langues prises en charge dans le projet cité en référence comprennent l'anglais et le français canadien **4 pts =** les langues prises en charge dans le projet cité en référence comprennent l'anglais et le français **2 pts =** les langues prises en charge dans le projet cité en référence comprennent l'anglais ou le français, mais pas les deux **0 pt** = les langues prises en charge dans le projet cité en référence ne comprennent ni l'anglais ni le français ou aucune réponse comparable.	
4	Le répondant devrait préciser l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence.	10 %	Les points seront attribués de la manière suivante : **5 pts** = le fournisseur de solutions proposé pour ce projet de SC est l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence **0 pt** = le fournisseur de solutions proposé pour ce projet de SC n'est pas l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence ou aucune réponse comparable.	

Références de déploiement de solutions logicielles précédentes – Référence 1				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
5	Le répondant devrait préciser l'organisation qui a fourni des services de soutien opérationnel continu à l'appui du projet cité en référence.	10 %	Les points seront attribués de la manière suivante : **5 pts** = le fournisseur de solutions proposé pour ce projet de SC est l'organisation qui a fourni les services de soutien opérationnel continu à l'appui du projet cité en référence **0 pt** = le fournisseur de solutions proposé pour ce projet de SC n'est pas l'organisation qui a fourni les services de soutien opérationnel continu à l'appui du projet cité en référence ou aucune réponse comparable.	
6	Le projet cité en référence devrait comprendre le déploiement des éléments suivants : 1. Gestion des nouveaux dossiers comme il est défini dans l'annexe B, section 3.2.1. 2. Gestion des cas comme il est défini dans l'annexe B, section 3.2.2. 3. Assurance qualité comme il est défini dans l'annexe B, section 3.2.3. 4. Gestion des prestataires de services comme il est défini dans l'annexe B, section 3.2.4. 5. Gestion des aiguillages comme il est défini dans l'annexe B, section 3.2.5. 6. Gestion des comptes de l'organisation comme il est défini dans l'annexe B, section 3.2.6. 7. Administration financière comme il est défini dans l'annexe B, section 3.2.9. 8. Gestion des rapports comme il est défini dans l'annexe B, section 3.2.11. 9. Gestion des utilisateurs comme il est défini dans l'annexe B, section 3.2.12. 10. Services du portail comme il est défini dans l'annexe B, section 3.2.13. 11. Gestion de la communication comme il est défini dans l'annexe B, section 3.2.14. 12.	20 %	Les points seront attribués de la manière suivante : **5 pts** = le projet cité en référence comprenait le déploiement de 10 ou plus des points 1 à 11. **4 pts** = le projet cité en référence comprenait le déploiement de 8 ou 9 des points 1 à 11. **3 pts** = le projet cité en référence comprenait le déploiement de 7 des points 1 à 11. **2 pts** = le projet cité en référence comprenait le déploiement de 6 des points 1 à 11. **1 pt** = le projet cité en référence comprenait le déploiement de 4 ou 5 des points 1 à 11. **0 pt** = le projet cité en référence comprenait le déploiement de moins de 4 des points 1 à 11 ou ne fournit pas de réponse pertinente.	

Références de déploiement de solutions logicielles précédentes – Référence 1				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
7	Le répondant devrait indiquer le nombre de cas* traités annuellement par le SGIPAE déployé. *Un « cas » est un client admissible au PAE orienté vers un conseiller en pratique privée accrédité.	10 %	Les points seront attribués de la manière suivante : **5 pts** = ≥ 20 000 cas par an **4 pts** = ≥ 10 00l0 à < 20 000 cas par an **3 pts**= ≥ 5 000 à < 10 000 cas par an **2 pts** = ≥ 3 000 à < 5 000 cas par an **1 pt** = ≥ 1 000 à < 3 000 cas par an **0 pt** = < 1 000 cas par an ou pas de réponse comparable.	

Référence 2

Répondant	
Client	
Nom de la personne ressource	
Titre de la personne ressource	
Numéro de téléphone	
Nom du projet	
Bref aperçu du projet	
Échéancier du projet	

Références de déploiement de solutions logicielles précédentes – Référence 2				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
1	Le répondant devrait indiquer que le SGIPAE de base fourni, déployé et exploité dans le cadre du projet cité en référence fonctionne à l'aide des modules logiciels et aux niveaux d'édition proposés.	25 %	Les points seront attribués de la manière suivante : **5 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels et aux niveaux d'édition proposés. **4 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels proposés à des niveaux d'édition qui ne sont pas à plus d'un niveau d'édition majeur avant le niveau d'édition actuel. **3 pts =** le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels proposés à des niveaux d'édition qui ne sont pas à plus de deux niveaux d'édition majeurs avant le niveau d'édition actuel. **2 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne en utilisant les modules logiciels proposés à des niveaux d'édition qui sont à plus de deux niveaux d'édition majeurs avant le niveau d'édition actuel **0 pt** = le SGIPAE de base fourni et déployé dans le projet cité en référence ne fonctionne pas à l'aide des modules logiciels proposés ou aucune réponse comparable.	
2	Le répondant devrait indiquer la date à laquelle le projet de préférence est entré en production réelle avec le SGIPAE. Par souci de clarté, le SGIPAE est entré en production réelle lorsque les fonctionnalités / modules suivants sont passés au mode de production réelle : 1. Gestion des nouveaux dossiers comme il est défini dans l'annexe B, section 3.2.1. 2. Gestion des cas comme il est défini dans l'annexe B, section 3.2.2.	10 %	Les points seront attribués de la manière suivante : **5 pts** = ≥ 36 mois avant la date de clôture de l'IQ **4 pts** = < 36 mois à ≥ 24 mois avant la date de clôture de l'IQ **3 pts** = < 24 mois à ≥ 12 mois avant la date de clôture de l'IQ **2 pts** = < 12 mois avant la date de clôture de l'IQ **0 pt** = pas en production réelle ou pas de réponse comparable.	

Références de déploiement de solutions logicielles précédentes – Référence 2				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
	3. Assurance qualité comme il est défini dans l'annexe B, section 3.2.3. 4. Gestion des prestataires de services comme il est défini dans l'annexe B, section 3.2.4. 5. Gestion des aiguillages comme il est défini dans l'annexe B, section 3.2.5. 6. Gestion des comptes de l'organisation comme il est défini dans l'annexe B, section 3.2.6. 7. Administration financière comme il est défini dans l'annexe B, section 3.2.11.			
3	Le répondant devrait préciser les langues prises en charge dans le projet cité en référence, les langues en question devant inclure l'anglais et le français.	15 %	Les points seront attribués de la manière suivante : **5 pts** = les langues prises en charge dans le projet cité en référence comprennent l'anglais et le français canadien **4 pts =** les langues prises en charge dans le projet cité en référence comprennent l'anglais et le français **2 pts =** les langues prises en charge dans le projet cité en référence comprennent l'anglais ou le français, mais pas les deux **0 pt** = les langues prises en charge dans le projet cité en référence ne comprennent ni l'anglais ni le français ou aucune réponse comparable.	
4	Le répondant devrait préciser l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence.	10 %	Les points seront attribués de la manière suivante : **5 pts** = le fournisseur de solutions proposé pour ce projet de SC est l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence **0 pt** = le fournisseur de solutions proposé pour ce projet de SC n'est pas l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence ou aucune réponse comparable.	

Références de déploiement de solutions logicielles précédentes – Référence 2				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
5	Le répondant devrait préciser l'organisation qui a fourni des services de soutien opérationnel continu à l'appui du projet cité en référence.	10 %	Les points seront attribués de la manière suivante : **5 pts** = le fournisseur de solutions proposé pour ce projet de SC est l'organisation qui a fourni les services de soutien opérationnel continu à l'appui du projet cité en référence **0 pt** = le fournisseur de solutions proposé pour ce projet de SC n'est pas l'organisation qui a fourni les services de soutien opérationnel continu à l'appui du projet cité en référence ou aucune réponse comparable.	
6	Le projet cité en référence devrait comprendre le déploiement des éléments suivants : 1. Gestion des nouveaux dossiers comme il est défini dans l'annexe B, section 3.2.1. 2. Gestion des cas comme il est défini dans l'annexe B, section 3.2.2. 3. Assurance qualité comme il est défini dans l'annexe B, section 3.2.3. 4. Gestion des prestataires de services comme il est défini dans l'annexe B, section 3.2.4. 5. Gestion des aiguillages comme il est défini dans l'annexe B, section 3.2.5. 6. Gestion des comptes de l'organisation comme il est défini dans l'annexe B, section 3.2.6. 7. Administration financière comme il est défini dans l'annexe B, section 3.2.9. 8. Gestion des rapports comme il est défini dans l'annexe B, section 3.2.11. 9. Gestion des utilisateurs comme il est défini dans l'annexe B, section 3.2.12. 10. Services du portail comme il est défini dans l'annexe B, section 3.2.13. 11. Gestion de la communication comme il est défini dans l'annexe B, section 3.2.14.	20 %	Les points seront attribués de la manière suivante : **5 pts** = le projet cité en référence comprenait le déploiement de 10 ou plus des points 1 à 11. **4 pts** = le projet cité en référence comprenait le déploiement de 8 ou 9 des points 1 à 11. **3 pts** = le projet cité en référence comprenait le déploiement de 7 des points 1 à 11. **2 pts** = le projet cité en référence comprenait le déploiement de 6 des points 1 à 11. **1 pt** = le projet cité en référence comprenait le déploiement de 4 ou 5 des points 1 à 11. **0 pt** = le projet cité en référence comprenait le déploiement de moins de 4 des points 1 à 11 ou ne fournit pas de réponse pertinente.	

Références de déploiement de solutions logicielles précédentes – Référence 2				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
7	Le répondant devrait indiquer le nombre de cas* traités annuellement par le SGIPAE déployé. *Un « cas » est un client admissible au PAE orienté vers un conseiller en pratique privée accrédité.	10 %	Les points seront attribués de la manière suivante : **5 pts** = ≥ 20 000 cas par an **4 pts** = ≥ 10 00l0 à < 20 000 cas par an **3 pts**= ≥ 5 000 à < 10 000 cas par an **2 pts** = ≥ 3 000 à < 5 000 cas par an **1 pt** = ≥ 1 000 à < 3 000 cas par an **0 pt** = < 1 000 cas par an ou pas de réponse comparable.	

Formulaire C-2 Références des services liés au projet de mise en œuvre du SGIPAE

Instructions pour remplir le formulaire :

1. Deux (2) exemples de projets pertinents doivent être fournis.
2. Un formulaire distinct de Références des services liés au projet de mise en œuvre du SGIPAE doit être rempli pour chaque exemple de projet.
3. Les réponses seront utilisées pour classer les références fournies en réponse au critère O-9 (Références des fournisseurs du SGIPAE).

Référence 1

Répondant	
Client	
Nom de la personne ressource	
Titre de la personne ressource	
Numéro de téléphone	
Nom du projet	
Bref aperçu du projet	
Échéancier du projet	

Références des services liés au projet de mise en œuvre du SGIPAE – Référence 1				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
1	Le répondant devrait décrire le SGIPAE de base fourni et déployé dans le cadre du projet cité en référence, incluant les modules logiciels et les niveaux d'édition proposés.	15 %	Les points seront attribués de la manière suivante : **5 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels et aux niveaux d'édition proposés. **4 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels proposés à des niveaux d'édition qui ne sont pas à plus d'un niveau d'édition majeur avant le niveau d'édition actuel. **3 pts =** le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels proposés à des niveaux d'édition qui ne sont pas à plus de deux niveaux d'édition majeurs avant le niveau d'édition actuel. **2 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne en utilisant les modules logiciels proposés à des niveaux d'édition qui sont à plus de deux niveaux d'édition majeurs avant le niveau d'édition actuel **0 pt** = le SGIPAE de base fourni et déployé dans le projet cité en référence ne fonctionne pas à l'aide des modules logiciels proposés ou aucune réponse comparable.	
2	Le répondant doit indiquer la date à laquelle le projet de préférence est entré en production réelle avec le SGIPAE. Par souci de clarté, le SGIPAE est entré en production réelle lorsque les fonctionnalités / modules suivants sont passés au mode de production réelle : 1. Gestion des nouveaux dossiers comme il est défini dans l'annexe B, section 3.2.1.	15 %	Les points seront attribués de la manière suivante : **5 pts** = ≥ 36 mois avant la date de clôture de l'IQ **4 pts** = < 36 mois à ≥ 24 mois avant la date de clôture de l'IQ **3 pts** = < 24 mois à ≥ 12 mois avant la date de clôture de l'IQ **2 pts** = < 12 mois avant la date de clôture de l'IQ **0 pt** = pas en production réelle ou pas de réponse comparable.	

Références des services liés au projet de mise en œuvre du SGIPAE – Référence 1				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
	2. Gestion des cas comme il est défini dans l'annexe B, section 3.2.2. 3. Assurance qualité comme il est défini dans l'annexe B, section 3.2.3. 4. Gestion des prestataires de services comme il est défini dans l'annexe B, section 3.2.4. 5. Gestion des aiguillages comme il est défini dans l'annexe B, section 3.2.5. 6. Gestion des comptes de l'organisation comme il est défini dans l'annexe B, section 3.2.6. 7. Administration financière comme il est défini dans l'annexe B, section 3.2.11.			
3	Le répondant devrait préciser les langues prises en charge dans le projet cité en référence, les langues en question devant inclure l'anglais et le français.	20 %	Les points seront attribués de la manière suivante : **5 pts** = les langues prises en charge dans le projet cité en référence comprennent l'anglais et le français canadien **4 pts =** les langues prises en charge dans le projet cité en référence comprennent l'anglais et le français **2 pts =** les langues prises en charge dans le projet cité en référence comprennent l'anglais ou le français, mais pas les deux **0 pt** = les langues prises en charge dans le projet cité en référence ne comprennent ni l'anglais ni le français ou aucune réponse comparable.	
4	Le répondant devrait préciser l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence.	25 %	Les points seront attribués de la manière suivante : **5 pts** = le fournisseur de solutions proposé pour ce projet de SC est l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence **0 pt** = le fournisseur de solutions proposé pour ce	

Références des services liés au projet de mise en œuvre du SGIPAE – Référence 1				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
			projet de SC n'est pas l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence ou aucune réponse comparable.	
5	Le répondant devrait préciser l'organisation qui a fourni des services de soutien opérationnel continu à l'appui du projet cité en référence.	25 %	Les points seront attribués de la manière suivante : **5 pts** = le fournisseur de solutions proposé pour ce projet de SC est l'organisation qui a fourni les services de soutien opérationnel continu à l'appui du projet cité en référence **0 pt** = le fournisseur de solutions proposé pour ce projet de SC n'est pas l'organisation qui a fourni les services de soutien opérationnel continu à l'appui du projet cité en référence ou aucune réponse comparable.	

Référence 2

Répondant	
Client	
Nom de la personne ressource	
Titre de la personne ressource	
Numéro de téléphone	
Nom du projet	
Bref aperçu du projet	
Échéancier du projet	

Références des services liés au projet de mise en œuvre du SGIPA – Référence 2				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
1	Le répondant devrait décrire le SGIPAE de base fourni et déployé dans le cadre du projet cité en référence, incluant les modules logiciels et les niveaux d'édition proposés.	15 %	Les points seront attribués de la manière suivante : **5 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels et aux niveaux d'édition proposés. **4 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels proposés à des niveaux d'édition qui ne sont pas à plus d'un niveau d'édition majeur avant le niveau d'édition actuel. **3 pts =** le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne à l'aide des modules logiciels proposés à des niveaux d'édition qui ne sont pas à plus de deux niveaux d'édition majeurs avant le niveau d'édition actuel. **2 pts** = le SGIPAE de base fourni et déployé dans le projet cité en référence fonctionne en utilisant les modules logiciels proposés à des niveaux d'édition qui sont à plus de deux niveaux d'édition majeurs avant le niveau d'édition actuel **0 pt** = le SGIPAE de base fourni et déployé dans le projet cité en référence ne fonctionne pas à l'aide des modules logiciels proposés ou aucune réponse comparable.	
2	Le répondant devrait indiquer la date à laquelle le projet de préférence est entré en production réelle avec le SGIPAE. Par souci de clarté, le SGIPAE est entré en production réelle lorsque les fonctionnalités / modules suivants sont passés au mode de production réelle : 1. Gestion des nouveaux dossiers comme il est défini dans l'annexe B, section 3.2.1. 2. Gestion des cas comme il est défini dans l'annexe B, section 3.2.2.	15 %	Les points seront attribués de la manière suivante : **5 pts** = ≥ 36 mois avant la date de clôture de l'IQ **4 pts** = < 36 mois à ≥ 24 mois avant la date de clôture de l'IQ **3 pts** = < 24 mois à ≥ 12 mois avant la date de clôture de l'IQ **2 pts** = < 12 mois avant la date de clôture de l'IQ **0 pt** = pas en production réelle ou pas de réponse comparable.	

Références des services liés au projet de mise en œuvre du SGIPA – Référence 2				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
	3. Assurance qualité comme il est défini dans l'annexe B, section 3.2.3. 4. Gestion des prestataires de services comme il est défini dans l'annexe B, section 3.2.4. 5. Gestion des aiguillages comme il est défini dans l'annexe B, section 3.2.5. 6. Gestion des comptes de l'organisation comme il est défini dans l'annexe B, section 3.2.6. 7. Administration financière comme il est défini dans l'annexe B, section 3.2.11.			
3	Le répondant devrait préciser les langues prises en charge dans le projet cité en référence, les langues en question devant inclure l'anglais et le français.	20 %	Les points seront attribués de la manière suivante : **5 pts** = les langues prises en charge dans le projet cité en référence comprennent l'anglais et le français canadien **4 pts =** les langues prises en charge dans le projet cité en référence comprennent l'anglais et le français **2 pts =** les langues prises en charge dans le projet cité en référence comprennent l'anglais ou le français, mais pas les deux **0 pt** = les langues prises en charge dans le projet cité en référence ne comprennent ni l'anglais ni le français ou aucune réponse comparable.	
4	Le répondant devrait préciser l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence.	25 %	Les points seront attribués de la manière suivante : **5 pts** = le fournisseur de solutions proposé pour ce projet de SC est l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence **0 pt** = le fournisseur de solutions proposé pour ce projet de SC n'est pas l'organisation qui a fourni les services de mise en œuvre à l'appui du projet cité en référence ou aucune réponse comparable.	

Références des services liés au projet de mise en œuvre du SGIPA – Référence 2				
N°	**Critères**	**Pondération**	**Méthode de notation**	**Réponse**
5	Le répondant devrait préciser l'organisation qui a fourni des services de soutien opérationnel continu à l'appui du projet cité en référence.	25 %	Les points seront attribués de la manière suivante : **5 pts** = le fournisseur de solutions proposé pour ce projet de SC est l'organisation qui a fourni les services de soutien opérationnel continu à l'appui du projet cité en référence **0 pt** = le fournisseur de solutions proposé pour ce projet de SC n'est pas l'organisation qui a fourni les services de soutien opérationnel continu à l'appui du projet cité en référence ou aucune réponse comparable.	

Appendice B de l'annexe C : Pondérations applicables aux critères d'évaluation cotés

EXIGENCES COTÉES DE L'IQ		
Hiérarchie	**Critères**	**Pondération globale**
C-1	**Répondant – Capacité organisationnelle**	**30 %**
C-1.1	Compréhension des exigences du projet de SAE	3 %
C-1.2	Maturité organisationnelle du répondant – Années	4,5 %
C-1.3	Profil du répondant – Organisation de prestation de services du SGIPAE de base	4,5 %
C-1.4	Profil du répondant – Portefeuille de services du fournisseur du SGIPAE de base	9 %
C-1.5	Maturité organisationnelle du répondant – Projets de déploiement du fournisseur du SGIPAE	9 %
C-2	**Solution logicielle de PAE proposée**	**40 %**
C-2.1	Solution proposée – Fonctionnalité de la solution de base	16 %
C-2.2	Solution proposée – Architecture de la solution	12 %
C-2.3	Solution proposée – Options de déploiement	12 %
C-3	**Sécurité et accessibilité**	**10 %**
C-3.1	Sécurité de projet – Politique de sécurité	5 %
C-3.2	Accessibilité	5 %
C-4	**Références**	**20 %**
C-4.1	Annexe C-1 Référence nº 1de déploiement de solutions logicielles précédentes	5 %
C-4.2	Annexe C-1 Référence nº 2 de déploiement de solutions logicielles précédentes	5 %
C-4.3	Annexe C-2 Référence nº 1 des services liés au projet de mise en œuvre du SGIPAE	5 %
C-4.4	Annexe C-2 Référence nº 2 des services liés au projet de mise en œuvre du SGIPAE	5 %

ANNEXE D

ÉBAUCHE D'EXIGENCES DE SÉCURITÉ APPLICABLES AUX SOLUTIONS SUR SITE AU STADE DE LA DEMANDE DE SOUMISSIONS ET À TOUT CONTRAT SUBSÉQUENT

Note: Ces exigences décrivent certaines, mais pas nécessairement toutes les exigences que le Canada a l'intention de traiter dans la Demande de soumissions (DDS). Des exigences relatives à la sécurité supplémentaires peuvent être incluses dans les phases ultérieures de ce processus d'approvisionnement. Le Canada inclut ces exigences dans la présente IQ afin d'informer les répondants à l'avance de certaines des exigences susceptibles d'être incluses dans la DDS connexe.

1. Avant l'attribution d'un contrat, les conditions suivantes doivent être remplies:

   (a) le soumissionnaire doit détenir une habilitation de sécurité d'organisme valide tel qu'indiqué ci-dessous;

   (b) les personnes proposées par le soumissionnaire qui ont besoin d'accéder à des informations, des actifs ou des chantiers sensibles classés ou protégés doivent répondre aux exigences de sécurité indiquées ci-dessous;

   (c) le soumissionnaire doit fournir le nom de toutes les personnes qui auront besoin d'accéder à des informations, actifs ou sites de travail sensibles ou protégés.

2. Dans le cas d'un soumissionnaire de coentreprise, chaque membre de la coentreprise doit satisfaire aux exigences de sécurité.

3. On rappelle aux soumissionnaires d'obtenir rapidement la cote de sécurité requise. Tout retard dans l'attribution d'un contrat pour permettre au soumissionnaire retenu d'obtenir l'autorisation requise sera à l'entière discrétion de l'autorité contractante.

4. Pour de plus amples renseignements sur les exigences en matière de sécurité, les soumissionnaires devraient consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

5. Les soumissionnaires étrangers doivent provenir d'un pays où il existe un accord bilatéral de sécurité industrielle avec le Canada qui stipule des équivalences de sécurité. Les soumissionnaires étrangers (y compris les États-Unis) doivent contacter l'autorité contractante pour obtenir les conditions des exigences de

sécurité qui s'appliqueront à la demande de soumissions et au contrat subséquent.

EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:

1. L'entrepreneur doit détenir en permanence, pendant l'exécution du contrat, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau **PROTÉGÉ B,** délivrées par le Programme de sécurité des contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC).

2. Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens **PROTÉGÉS**, ou à des établissements dont l'accès est réglementé, doivent TOUS détenir une cote de FIABILITÉ en vigueur, délivrée ou approuvée par le PSC, TPSGC.

3. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données au niveau **PROTÉGÉ** tant que le PSC, TPSGC ne lui en aura pas donné l'autorisation par écrit. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau **PROTÉGÉ B.**

4. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable du PSC, TPSGC.

5. L'entrepreneur ou l'offrant doit se conformer aux dispositions des documents suivants :

   a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité, reproduite ci-joint à l'Annexe E;

   b) le *Manuel de la sécurité industrielle* (dernière édition).

ANNEXE E

LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat: HT300-193651

Security Classification / Classification de sécurité

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Health Canada

2. Branch or Directorate / Direction générale ou Direction: CSB / Specialized Health Services Directorate / EAS

3. a) Subcontract Number / Numéro du contrat de sous-traitance

3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Invitation To Qualify (ITQ) for a ready to use Commercial-Off-The-Shelf (COTS) software that fits the business needs of the Employee Assistance Services (EAS) group.

5. a) Will the supplier require access to Controlled Goods? / Le fournisseur aura-t-il accès à des marchandises contrôlées? — [✓] No / Non [ ] Yes / Oui

5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? / Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? — [✓] No / Non [ ] Yes / Oui

6. Indicate the type of access required / Indiquer le type d'accès requis
Access to development servers limited or brokered by Shared Services Canada (SSC) for installation of Employee Assistance Program Info. Mgmt. System (EAPIMS) software for configuration and testing purposes.

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? / Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) / (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) — [ ] No / Non [✓] Yes / Oui

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. / Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. — [✓] No / Non [ ] Yes / Oui

6. c) Is this a commercial courier or delivery requirement with no overnight storage? / S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit? — [✓] No / Non [ ] Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada [✓]	NATO / OTAN [ ]	Foreign / Étranger [ ]

7. b) Release restrictions / Restrictions relatives à la diffusion

Canada	NATO / OTAN	Foreign / Étranger
No release restrictions / Aucune restriction relative à la diffusion [✓]	All NATO countries / Tous les pays de l'OTAN [ ]	No release restrictions / Aucune restriction relative à la diffusion [ ]
Not releasable / À ne pas diffuser [ ]		
Restricted to: / Limité à : [ ]	Restricted to: / Limité à : [ ]	Restricted to: / Limité à : [ ]
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

Canada	NATO / OTAN	Foreign / Étranger
PROTECTED A / PROTÉGÉ A [✓]	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ [ ]	PROTECTED A / PROTÉGÉ A [ ]
PROTECTED B / PROTÉGÉ B [✓]	NATO RESTRICTED / NATO DIFFUSION RESTREINTE [ ]	PROTECTED B / PROTÉGÉ B [ ]
PROTECTED C / PROTÉGÉ C [ ]	NATO CONFIDENTIAL / NATO CONFIDENTIEL [ ]	PROTECTED C / PROTÉGÉ C [ ]
CONFIDENTIAL / CONFIDENTIEL [ ]	NATO SECRET / NATO SECRET [ ]	CONFIDENTIAL / CONFIDENTIEL [ ]
SECRET / SECRET [ ]	COSMIC TOP SECRET / COSMIC TRÈS SECRET [ ]	SECRET / SECRET [ ]
TOP SECRET / TRÈS SECRET [ ]		TOP SECRET / TRÈS SECRET [ ]
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) [ ]		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) [ ]

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat: HT300-193651

Security Classification / Classification de sécurité

PART A (continued) / PARTIE A (suite)

6. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — [✓] No / Non [ ] Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — [✓] No / Non [ ] Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

[✓] RELIABILITY STATUS / COTE DE FIABILITÉ	[ ] CONFIDENTIAL / CONFIDENTIEL	[ ] SECRET / SECRET	[ ] TOP SECRET / TRÈS SECRET
[ ] TOP SECRET – SIGINT / TRÈS SECRET – SIGINT	[ ] NATO CONFIDENTIAL / NATO CONFIDENTIEL	[ ] NATO SECRET / NATO SECRET	[ ] COSMIC TOP SECRET / COSMIC TRÈS SECRET
[ ] SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux :

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — [✓] No / Non [ ] Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — [ ] No / Non [ ] Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — [ ] No / Non [✓] Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — [✓] No / Non [ ] Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — [✓] No / Non [ ] Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — [ ] No / Non [✓] Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — [✓] No / Non [ ] Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
HT300-193651
Security Classification / Classification de sécurité

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMO TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens	✓	✓														
Production																
IT Media / Support TI	✓	✓														
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
HT300-193651	
Security Classification / Classification de sécurité	

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Nishad Datoo	Project Manager	N. Datoo

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
(613) 949-6257		nishad.datoo@canada.ca	Jan. 27, 2020

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
SONIA LAROSE	Sec. Contract Coord.	Larose

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-954-1775		Sonia.larose@canada.ca	2020-01-28

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? / Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? ☐ No / Non ☑ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

ANNEXE F

EBAUCHE DES EXIGENCES DE SÉCURITÉ APPLICABLES AUX SOLUTIONS DE LOGICIELS-SERVICES AU STADE DE LA DEMANDE DE SOUMISSIONS ET DE TOUT CONTRAT SUBSÉQUENT

(a) L'annexe F fixe les exigences minimales de sécurité qui doivent être respectées afin de démontrer la conformité de la sécurité pour la fourniture du SGIPAE en utilisant la solution de Logiciel-service au stade de la demande de soumissions. Ces exigences décrivent certaines, mais pas nécessairement toutes les exigences que le Canada a l'intention de traiter dans la DDS. Des exigences relatives à la sécurité supplémentaires peuvent être incluses dans les phases ultérieures de ce processus d'approvisionnement. Le Canada inclut ces exigences dans la présente IQ afin d'informer les répondants à l'avance de certaines des exigences susceptibles d'être incluses dans la DDS connexe.

(b) L'annexe est divisée en 5 appendices comme suit:

- Appendice A - Exigences relatives au programme de sécurité industrielle pour les besoins en infonuagique au niveau Protégé B
- Appendice B - Exigences de conformité en matière de sécurité des données au niveau Protégé B
- Appendice C - Obligations en matière de protection de la vie privée
- Appendice D - Obligations en matière de sécurité
- Appendice E - Processus d'intégrité de la chaîne d'approvisionnement

Appendice A – Exigences relatives au Programme de sécurité industrielle pour les besoins en infonuagique au niveau Protégé B

1. Avant l'attribution d'un contrat, les conditions suivantes doivent être remplies :

   (a) le contractant doit être titulaire d'une habilitation de sécurité d'organisation valable, comme indiqué ci-dessous;

   (b) les personnes proposées par le contractant/sous-traitant qui doivent avoir accès à des informations ou à des biens classifiés ou protégés ou à des sites de travail sensibles doivent satisfaire aux exigences de sécurité indiquées ci-dessous ;

   (c) le contractant doit fournir le nom de toutes les personnes qui auront besoin d'accéder à des informations ou à des biens classifiés ou protégés ou à des sites de travail sensibles.

2. Dans le cas d'une coentreprise Entrepreneur, chaque membre de la coentreprise doit satisfaire aux exigences de sécurité.

3. Il est rappelé aux contractants d'obtenir rapidement l'autorisation de sécurité requise. Tout retard dans l'attribution d'un contrat pour permettre à l'entrepreneur retenu d'obtenir l'habilitation requise sera à l'entière discrétion de l'autorité contractante.

4. Pour de plus amples renseignements sur les exigences en matière de sécurité, l'entrepreneur doit consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html).

A.1 Exigence en matière de sécurité pour entrepreneur canadien

1. L'entrepreneur doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ B**,** délivrées par la Secteur de la Sécurité Industrielle (SSI) de **Travaux publics et Services gouvernementaux Canada (TPSGC).**

2. Les membres du personnel de l'entrepreneur devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau FIABILITE, délivrée ou approuvée par la SSI de **TPSGC**.

3. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements au niveau PROTÉGÉ jusqu'à ce que l'autorisation écrite a été émise par l'autorité en matière de sécurité pour le ministère. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau PROTÉGÉ A et B incluant un lien électronique au niveau PROTÉGÉ A et B.

4. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de la SSI de **TPSGC**.

5. L'entrepreneur doit se conformer aux dispositions des documents suivants :

   a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'annexe E;

   b) le Manuel de la sécurité industrielle (dernière édition);

   c) Site Web du SSI : Exigences de sécurité des contrats du gouvernement du Canada, veuillez visitez https://www.tpsgc-pwgsc.gc.ca/esc-src

A.2 Exigence relatives à la sécurité pour les entrepreneurs étrangers

L'Autorité désignée en matière de sécurité pour le Canada (ADS canadien) pour les questions industrielles au Canada est la Direction de la sécurité industrielle internationale (DSII), Secteur de la sécurité industrielle (SSI), Travaux publics et Services gouvernementaux Canada (TPSGC). L'ADS canadien est chargée d'évaluer la conformité des soumissionnaires aux exigences en matière de sécurité pour l'entrepreneur/sous-traitant étrangers. Les exigences en matière de sécurité suivantes s'appliquent à l'entrepreneur/sous-traitant étranger destinataire, incorporés ou autorisés à faire des affaires dans un état autre que le Canada et qui assurent la prestation de services décrites dans l'énoncé des travaux ultérieur et s'ajoute aux exigences de confidentialité et de sécurité de l'appendice C et l'appendice D.

1. **L'entrepreneur/Le sous-traitant** étranger destinataire doit être dans un pays de l'Union européenne, dans un pays de l'organisation du traité de l'Atlantique Nord (OTAN) ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité et un protocole d'entente bilatérale ou multinationale. Le programme de sécurité a des ententes en matière de sécurité et protocole d'entente bilatérale ou multinationale avec les pays mentionnés au site de SPAC suivant: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html.

2. **L'entrepreneur/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution du **contrat/sous-traitance**, tenir une équivalence à une vérification d'organisation désignée (VOD), délivrée par l'ADS canadien comme suit :

   (a) **L'entrepreneur/Le sous-traitant** étranger destinataire doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence.

   (b) L'entrepreneur/Le sous-traitant étranger destinataire ne doit pas entreprendre les travaux, fournir les services ou assurer toute autre prestation tant que l'Administration désignée en matière de sécurité au Canada (ADS canadien) n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le **contrat/sous-traitance**. L'ADS canadien donne cette confirmation par écrit **à l'entrepreneur/au sous-traitant** étranger destinataire. Un Formulaire d'attestation remis par l'ADS canadien **à l'entrepreneur/au sous-traitant** étranger destinataire permettra de confirmer la conformité et l'autorisation de fournir les services prévus.

   (c) L'entrepreneur/Le sous-traitant étranger destinataire proposé doit identifier l'agent de sécurité du contrat (ASC) autorisé et un agent remplaçant de sécurité d'entreprise (ARSE) (le cas échéant) qui sera responsable du contrôle des exigences de sécurité, telles qu'elles sont définies dans le **contrat/sous-traitance**. Cette personne sera désignée par le président-directeur général ou par un cadre supérieur clé de l'entreprise étrangère destinataire proposée. Les cadres supérieurs clés comprennent les propriétaires, les agents, les directeurs, les cadres et les partenaires occupant un poste qui leur permettrait d'avoir une influence sur les politiques ou les pratiques de l'organisation durant l'exécution du contrat.

   (d) L'entrepreneur/Le sous-traitant étranger destinataire n'autorisera pas l'accès à des renseignements/biens de niveau **PROTÉGÉ du Canada**, sauf à son personnel ayant été évalué conformément à la définition et aux pratiques énoncées dans la Norme relative au filtrage de sécurité du Conseil du Trésor (https://www.tbssct.gc.ca/pol/doc-fra.aspx?id=28115) ou à l'utilisation de mesures équivalentes acceptables établies par l'entrepreneur/le sous-traitant dans leur documentation accessible au public, et comme convenu par le Canada.

3. Les renseignements/biens de niveau **CANADA PROTÉGÉ** fournis ou produits dans le cadre **du contrat/sous-traitance** ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants:
   (a) L'ADS canadien atteste par écrit que le sous-traitant étranger destinataire a obtenu l'accès aux renseignements/biens de niveau **CANADA PROTÉGÉ** par l'intermédiaire de l'ADS canadien;
   (b) L'ADS canadien donne son autorisation écrite lorsque l'autre sous-traitant étranger destinataire est situé dans un autre pays.

4. **L'entrepreneur/Le sous-traitant** étranger destinataire NE DOIT PAS emporter de renseignements/ biens de niveau **CANADA PROTÉGÉ** hors des établissements de travail visés, et **l'entrepreneur/ sous-traitant** étranger destinataire doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.

5. **L'entrepreneur/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements/biens de niveau **CANADA PROTÉGÉ** pour répondre à des besoins distincts de l'exécution du **contrat/sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de auprès de l'ADS canadien.

6. **L'entrepreneur/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements/biens de niveau **CANADA PROTÉGÉ** pour répondre à des besoins distincts de l'exécution du **contrat/sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de auprès de l'ADS canadien.

7. Les contrats de sous-traitance comportant des exigences de sécurité NE DOIVENT PAS être attribués sans l'autorisation écrite préalable de la DSA canadienne.

8. **L'entrepreneur/Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité attaché à l'annexe E pour les exigences de nuages au niveau protégé B.

9. Le Canada a le droit de rejeter toute demande faite séparément et indépendamment de l'autorisation prévue dans le présent contrat en ce qui concerne l'entrepreneur/sous-traitant qui fournit les services d'accéder, de traiter, de produire, de transmettre ou de stocker par voie électronique des renseignements/biens PROTÉGÉS PAR LE CANADA liés aux travaux dans tout autre pays s'il y a des raisons de s'inquiéter de la sécurité, de la confidentialité ou de l'intégrité des renseignements.

Appendice B – Exigences de conformité en matière de sécurité des données au niveau protégées B

Les vingt (20) exigences de sécurité suivantes, doivent être respectées afin de démontrer la conformité à la sécurité (**jusqu'à et y compris les données protégées B**).

Table 1. Exigences pour la conformité de la sécurité des données protégées B

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
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. b) 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

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
			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. 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	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

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
		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 : 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; 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, validé par deux formes d'identification; f) l'escorte des visiteurs et la surveillance de leurs activités; g) la tenue de registres de vérification de l'accès physique; h) le contrôle et la gestion des dispositifs d'accès physique;	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
		i) l'application de mesures de protection des données du Canada à d'autres lieux de travail (p. ex., les sites 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 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: (a) la séparation entre l'administration interne du fournisseur et les ressources utilisées par ses clients; et (b) 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.	Le fournisseur doit fournir une documentation démontrant que le fournisseur des services proposés se conforme aux exigences.
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	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 :

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
		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 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 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	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, 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,	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 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
		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; 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, validé par deux formes d'identification; f) l'escorte des visiteurs et la surveillance de leurs activités; 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 de mesures de protection des données du GC à d'autres lieux de travail (p. ex., les sites 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 d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.	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
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; 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 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
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 oeuvre 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 services de la TI du GC fondés sur l'informatique en nuage pour 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 au moyen du processus d'évaluation de la sécurité des technologies de l'information (TI) du fournisseur de services infonuagiques (CSP) du Centre canadien pour la cybersécurité (CCCS) (ITSM.50.100) (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux). Tout fournisseur qui a participé au processus doit fournir de la documentation confirmant qu'il a terminé le processus d'intégration avec (i) une copie du plus récent rapport d'évaluation rempli fourni par le CCCS; et (ii) une copie du rapport sommaire le plus récent fourni par le CCCS. Cela accélérera le processus de qualification et, en même temps, n'oblige pas le fournisseur à démontrer la conformité. Pour les fournisseurs qui ont déjà complété l'évaluation en sécurité en fournissant au CCC les rapports de certification de sécurité SOC 2 Type II et qui ont déjà	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. 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 2) 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 3) 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; b) indiquer la raison sociale légale du fournisseur du logiciel-service commercialement disponible proposé et du fournisseur de services d'informatique en nuage; c) indiquer la date ou l'état de la certification actuelle; d) donner la liste des actifs, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification; e) 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

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
		conclu une entente de non divulgation (END) avec le CCC doivent transmettre leur certification et leurs rapports de certification directement au CCC à contact@cyber.gc.ca afin de se conformer à cette exigence. 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.	données, le rapport d'évaluation de l'organisation de sous-services doit être joint; et f) 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 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
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 la conformité aux exigences de sécurité sélectionnées dans le Profil de contrôle de sécurité du GC pour les services infonuagiques de TI du GC disponibles (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/services-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 applicables de l'industrie indiquées ci-dessous, et validée au moyen d'évaluations par des tiers indépendants. La cartographie des contrôles de sécurité doit être incluse; Profil de contrôle de sécurité du GC pour les services de TI du GC en nuage et Certification de l'industrie dans le cadre d'une assurance par un tiers détaillée au critère O8.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
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; (ii) des sous-traitants de sous-traitants du fournisseur en aval de la chaîne; iii) toute filiale. 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
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
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
O13	Confidentialité par conception	Le fournisseur doit démontrer qu'il met en œuvre une confidentialité par conception au cours du cycle de vie du développement de son logiciel, conformément au 'développement sécurisé', tel qu'énoncé ci-dessous : Développement sécurisé (1) 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 27034; (iii) ITSG-33; (iv) Safecode; (v) Open Web Application Security Project (OWASP) (p. ex. Application Security Verification Standard [ASVS] ou une norme équivalente approuvée par le Canada par écrit). (2) À la demande du Canada, le fournisseur doit fournir un document qui décrit le logiciel documenté de l'entrepreneur, ainsi que l'approche et le processus adoptés relativement au cycle de vie du développement du système.	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
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; c) exécuter et vérifier les autorisations d'accès aux services et aux actifs d'information; d) 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; e) 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; f) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier (palier 2 seulement) les utilisateurs finaux ayant un accès privilégié,	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
		conformément au document ITSP.30.031 V2 (ou versions ultérieures) du CST (https://www.cse-cst.gc.ca/fr/node/1842/html/26717); g) 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; 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 m) 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
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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
			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 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
			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, 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.	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 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.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité
O19	Fuite d'information	**Fuite d'information** (1) Le fournisseur doit avoir un processus documenté qui énonce son approche en cas d'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 ii) à une autre pratique exemplaire du secteur 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 : a) un processus d'identification des éléments de données précis utilisés dans la contamination d'un système; b) un processus visant à isoler et à éradiquer un système contaminé; c) un processus d'identification des systèmes pouvant avoir été subséquemment contaminés et toute autre mesure prise pour empêcher la propagation de la contamination; d) une confirmation d'une personne-ressource, de procédures appropriées et d'une entente concernant la communication sécurisée afin d'offrir de l'aide, si possible, aux administrateurs du service à la clientèle. (2) À la demande du Canada, le fournisseur doit fournir un document qui décrit le processus d'intervention en cas de fuite d'information du fournisseur.	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.

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. a) 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; b) 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); c) 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 d) 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.

Appendice C – Obligations en matière de protection de la vie privée

1. Généralités

Le système de gestion de l'information du programme d'aide aux employés (SGIPAE) ne sera pas utilisé pour stocker ou gérer des données cliniques ou médicales pouvant être identifiées avec une personne spécifique. Seuls les rapports et les données statistiques nécessaires à la gestion et à l'administration du programme seront conservés dans l'environnement EAPIMS. Toutes les données cliniques ou médicales seront détenues uniquement par les cliniciens qui fournissent des services et à qui les clients du programme ont été référés.

(a) Objectif

Le présent appendice a pour objet d'énoncer les obligations du fournisseur en ce qui concerne la configuration et la gestion appropriées des actifs et des actifs informationnels, afin de protéger ces actifs et ces actifs contre toute modification, accès ou exfiltration non autorisés, le tout conformément à l'engagement, la présente appendice, les mesures de sécurité spécifiques du fournisseur et les politiques canadiennes en matière de sécurité et de confidentialité (collectivement appelées **«obligations de sécurité et de confidentialité»**).

(b) Exécution des obligations en matière de protection de la vie privée

Les obligations du fournisseur contenues dans les présentes obligations de confidentialité doivent être transférées par le fournisseur aux sous-processeurs du fournisseur, dans la mesure où elles s'appliquent à chaque sous-processeur du fournisseur, étant donné la nature des services fournis au fournisseur.

(c) Gestion du changement

Le fournisseur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir à jour les obligations en matière de confidentialité afin de se conformer aux pratiques de la vie privée selon les normes de l'industrie, à condition que si ces modifications peuvent raisonnablement être prises en charge sans ressources supplémentaires, le fournisseur doit effectuer ces modifications sans frais supplémentaires pour le Canada (c.-à-d. via une demande de changement à coût nul).

Le fournisseur doit accepter d'informer le Canada de toutes les améliorations qui pourraient avoir une incidence sur les services dans le contrat, y compris les améliorations techniques, administratives ou tout autre type d'améliorations. Le fournisseur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier, sans supplément pour le Canada.

2. Reconnaissance

Les parties reconnaissent que:

a) Tous les biens et les actifs informationnels sont assujettis à ces obligations en matière de confidentialité.

b) Nonobstant toute autre disposition du présent appendice, les parties partagent la responsabilité d'élaboration et du maintien des politiques, des procédures et des contrôles de confidentialité relatifs aux biens et aux actifs informationnels.

c) Le fournisseur ne doit pas avoir ou tenter d'obtenir la garde d'un actif d'information, ni permettre à un membre du personnel des services à accéder à un actif information avant la mise en œuvre des obligations de confidentialité requises, comme l'exige présent appendice, au plus tard à l'attribution du marché.

3. Sécurisation des actifs informatiques

(a) Les données du Canada, y compris tous les renseignements personnels (RP), seront utilisées ou autrement traitées uniquement pour fournir au Canada les services, y compris à des fins compatibles avec la fourniture de ces services. Le fournisseur ne doit pas utiliser ou traiter autrement les données du Canada ni en tirer des informations à des fins publicitaires ou commerciales similaires. Entre les parties, le Canada conserve tous les droits, titres et intérêts dans et sur les données des clients. Le Fournisseur n'acquiert aucun droit sur les Données Client, à l'exception des droits que le Client accorde au Fournisseur de fournir les Services au Client.

4. Assurance des fournisseurs-tiers: certifications

(a) Le fournisseur doit s'assurer qu'en ce qui concerne les renseignements personnels qu'il peut héberger, stocker ou traiter sur tous les actifs, l'infrastructure du fournisseur (y compris tout service IaaS, PaaS ou SaaS fourni au Canada) et les emplacements de service sont conformes à l'industrie suivante certifications:

(i) ISO / IEC 27018: 2014 Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans les nuages publiques agissant en tant que processeurs PII - Certification obtenue par un organisme de certification accrédité.

(b) Le fournisseur doit démontrer la conformité à ces certifications en fournissant des rapports d'évaluation tiers indépendants ou des certifications pour toutes les parties du service.

(c) Chaque certification fournie doit: (i) identifier le nom commercial légal du fournisseur ou du sous-traitant fournisseur applicable; (ii) identifier la date de certification du fournisseur ou du sous-processeur fournisseur, y compris la date de certification du fournisseur

de services cloud et le statut de cette certification; (iii) identifier la liste des actifs, de l'infrastructure des fournisseurs et des emplacements de service dans le cadre du rapport de certification. Si la méthode spécifiée est utilisée pour exclure les organisations de sous-service telles que l'hébergement de centre de données, le rapport d'évaluation de l'organisation de sous-service doit être inclus.

(d) Chaque certification ISO fournie dans la présente section doit être valable pendant toute la durée du contrat, dans les 12 mois précédant le début du contrat. Les certifications doivent être accompagnées de rapports d'évaluation ISO à l'appui.

(e) (e) Le fournisseur doit maintenir la devise de sa certification selon les normes décrites au paragraphe 5 (1) tout au long du contrat. Le fournisseur doit fournir, au moins une fois par an et rapidement à la demande du Canada, tous les rapports ou dossiers qui peuvent être raisonnablement requis pour démontrer que les certifications du fournisseur restent à jour et sont valables pour la durée du contrat.

5. Respect de la vie privée

(a) Le fournisseur doit démontrer à travers le rapport d'évaluation par la partie indépendante et le rapport d'audit qui :

(i) limites la création, collection, réception, gestion, d'accès, possession, d'envoi, divulgation et disposition de l'information personnelle, et permettre uniquement dans la mesure de la nécessite pour exécuter le travail et,

(i) mis en place des processus et des contrôles de sécurité actualisés tels que les contrôles de gestion des accès, la sécurité des ressources humaines, la cryptographie et la sécurité physique, opérationnelle et des communications, afin de préserver l'intégrité, la confidentialité et l'exactitude de toutes les informations et données, ainsi que des métadonnées, quel que soit leur format.

(b) Ceci s'applique à toutes les informations, données et métadonnées en la possession du fournisseur ou sous sa responsabilité, acquises en vertu de, ou résultant de toute autre manière hors des responsabilités et obligations du contractant en vertu du contrat. L'entrepreneur reconnaît que cela est nécessaire pour que le Canada puisse compter sur les informations, les données et les métadonnées et pour qu'il puisse s'acquitter de ses propres obligations légales, y compris des obligations légales. Cela est également nécessaire pour garantir que les informations, les données et les métadonnées peuvent être utilisées comme preuves convaincantes devant un tribunal.

6. Audit de conformité

(a) Dans le cas où le Canada doit effectuer des audits de sécurité, des inspections et / ou examiner toute information appendice (par exemple, documentation, description de protection des données, architecture de données et descriptions de sécurité) conformément à la section 12.1, les deux parties conviennent de négocier une solution en bonne foi et de considérer à la fois la raison d'être de la demande du Canada et les processus et protocoles de l'entrepreneur.

(b) Dans les 30 jours suivant la demande de l'autorité contractante, l'entrepreneur doit faire appel à un tiers pour effectuer un audit de la protection de la vie privée ou fournir la preuve qu'il ne génère pas, ne collecte, n'utilise pas, ne stocke ou ne divulgue pas d'informations personnelles additionnelles, telles que définies par Le Canada, autre que les données du client telles que définies par l'entrepreneur, ne possède pas spécifiquement de données à caractère personnel dans les données de support (collectées dans des journaux (par exemple, des données de télémétrie telles que les en-têtes et le contenu d'un message électronique).

(c) The Le fournisseur doit effectuer les vérifications de confidentialité et de sécurité, de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter et protéger les biens et les actifs d'information, comme suit :

(i) Lorsqu'une norme ou un cadre prévoit des vérifications, une vérification de cette norme ou de ce cadre de contrôle sera entreprise au moins une fois par année;

(ii) Chaque vérification sera effectuée conformément aux normes et aux règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable; et

(iii) Chaque vérification sera effectuée par un vérificateur tiers qualifié et indépendant qui (i) est qualifié selon l'AICPA, CPA Canada ou le régime de certification ISO, et (ii) se conforme à la norme ISO/IEC 17 020 sur les systèmes de management de la qualité à la sélection et aux frais du fournisseur.

(d) Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être communiqué au Canada. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le vérificateur externe. Le fournisseur doit corriger rapidement et à la satisfaction du vérificateur les problèmes soulevés dans tout rapport de vérification et doit (i) fournir au Canada le plan pour corriger toute constatation négative découlant de ces rapports et (ii) fournir au Canada, sur demande, des rapports d'étape sur la mise en œuvre dans les dix (10) jours ouvrables du gouvernement fédéral.

(e) À la demande du Canada, le fournisseur ou un sous-traitant peut fournir des renseignements additionnels sur le fournisseur, y compris des plans de sécurité, des conceptions ou des documents d'architecture du système qui fournissent une description complète du système, afin de compléter les rapports de certification et de vérification décrits dans la présente et de démontrer la conformité du fournisseur avec les certifications requises de l'industrie.

7. 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 ;

(b) est conforme au cadre de gestion de la confidentialité et aux exigences de la politique spécifiées dans la norme ISO 29100; et

(c) Adhère à la confidentialité dès la conception des 7 principes fondamentaux (voir https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).

8. Demandes de propriété des données et de confidentialité

(a) Les données du client, y compris toutes les informations personnelles (PI), seront utilisées ou autrement traitées uniquement pour fournir les services, y compris à des fins compatibles avec la fourniture des services. L'entrepreneur ne doit en aucun cas utiliser ou traiter de données Canada ou en tirer des informations à des fins publicitaires ou à des fins commerciales similaires. Entre les parties, le client conserve tous les droits, titres et intérêts relatifs aux données du client. L'entrepreneur n'acquiert aucun droit dans les données du Canada, autres que les droits que le client accorde à l'entrepreneur pour fournir la solution au client.

(b) Toutes les données que l'entrepreneur stocke, héberge ou traite au nom du Canada demeurent la propriété du Canada. À la demande de l'autorité contractante, l'entrepreneur doit fournir des enregistrements de données personnelles dans les cinq jours ouvrables du gouvernement fédéral (ou sept jours ouvrables du gouvernement fédéral s'il est nécessaire de les récupérer à partir d'une sauvegarde / réplication hors site) dans un document Word ou Excel.

9. Agent de protection de la vie privée

(a) Dans les 10 jours suivant l'octroi du contrat, le fournisseur doit fournir au Canada les informations permettant d'identifier une personne, en tant qu'agent de la protection de la vie privée, qui agira en tant que représentant de l'entrepreneur pour toutes les questions liées aux informations personnelles et aux enregistrements. Le fournisseur doit fournir le nom et les coordonnées de cette personne, y compris son titre commercial, son adresse électronique et son numéro de téléphone.

10. Aider à la réalisation de l'évaluation des incidences sur la vie privée au Canada

(a) À la demande du responsable technique, l'entrepreneur doit aider le Canada à créer une évaluation des facteurs relatifs à la vie privée conformément à la Directive du Conseil du Trésor sur l'évaluation des facteurs relatifs à la vie privée (https://www.statcan.gc.ca/fra/about/pia). / dcpia) en aidant le Canada à fournir les documents justificatifs, y compris une EFVP fondamentale pour le Canada fournie par l'entrepreneur. L'entrepreneur accepte de fournir ce soutien dans les dix jours ouvrables suivant une demande ou dans un délai convenu par les parties en fonction de la complexité de la demande présentée par le Canada.

11. Atteinte à la vie privée

(a) L'entrepreneur doit alerter et informer promptement le responsable technique (par téléphone et par courriel) de toute compromission, violation ou tout élément de preuve la laissant croire raisonnablement que le risque de compromission, ou de violation, est imminent,

ou pourrait l'être, ou si les garanties existantes ont cessé de fonctionner, pendant la période suivante (7 jours x 24 heures x 365 jours) et dans les engagements de niveau de service du fournisseur de services nuages.

(b) Si l'entrepreneur prend connaissance d'une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des données sur le client ou à des informations personnelles lors du traitement par l'entrepreneur (chacun étant un «incident de sécurité»), le contractant doit promptement et sans retard indu:

(i) je. informer le Canada de l'incident de sécurité;
(ii) enquêter sur l'incident de sécurité et fournir au Canada des informations détaillées sur l'incident de sécurité; et
(iii) prendre des mesures raisonnables pour atténuer les effets et minimiser les dommages résultant de l'incident de sécurité.

(c) L'entrepreneur doit :

(i) Conserver un registre des violations de la sécurité avec une description de la violation, la période, les conséquences de la violation, le nom du journaliste et le destinataire de la violation, ainsi que la procédure de récupération des données; et

(ii) Suit ou permet au Canada de suivre les divulgations de données du Canada, y compris les données qui ont été divulguées, à qui et à quelle heure.

12. Propriété des renseignements personnels et des dossiers

(a) Pour exécuter les services et/ou les travaux, l'entrepreneur / sous-traitant destinataire étranger recevra et/ou collectera des informations personnelles de tiers. L'entrepreneur / sous-traitant destinataire étranger reconnaît qu'il n'a aucun droit sur les renseignements personnels ou les dossiers et que le Canada est propriétaire des dossiers. Sur demande, l'entrepreneur ou le sous-traitant destinataire étranger doit mettre immédiatement à la disposition du Canada tous les renseignements personnels et tous les dossiers dans un format acceptable par le Canada.

13. Utilisation des informations personnelles

(a) **L'entrepreneur / sous-traitant** étranger destinataire accepte de créer, collecter, recevoir, gérer, accéder, utiliser, conserver et éliminer les informations personnelles et les enregistrements uniquement pour exécuter les services et / ou les travaux conformément au contrat / sous-contrat.

14. Cueillette des renseignements personnels

(a) Si **l'entrepreneur/le sous-traitant** étranger destinataire doit obtenir des renseignements personnels d'un tiers dans le cadre des travaux, il ne doit recueillir que les renseignements personnels lui permettant d'exécuter les travaux. L'entrepreneur/Le sous-traitant étranger destinataire doit recueillir les renseignements personnels auprès de l'individu concerné et l'informer (au moment de la cueillette ou préalablement) de ce qui suit :

(i) les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;

(ii) les usages qui seront faits des renseignements personnels recueillis;

(iii) que la divulgation des renseignements personnels est volontaire ou, s'il existe une obligation juridique de divulguer les renseignements personnels, les fondements de cette obligation juridique;

(iv) les conséquences, s'il en est, du refus de fournir les renseignements;

(v) que l'intéressé au droit d'accéder à ses renseignements personnels et d'y apporter des corrections;

(vi) les renseignements personnels feront partie d'un fichier de renseignements personnels particulier (au sens de la Loi sur la protection des renseignements personnels), et fournir à l'individu de l'information concernant l'institution fédérale qui gère le fichier de renseignements personnels, si l'autorité contractante a fourni ces renseignements à l'entrepreneur/au sous-traitant étranger destinataire.

(b) L'entrepreneur, ses sous-traitants et leurs employés respectifs doivent s'identifier auprès des individus desquels ils recueillent des renseignements personnels et leur donner le moyen de vérifier qu'ils sont autorisés à recueillir les renseignements personnels en vertu d'un contrat passé avec le Canada.

(c) Si l'autorité contractante l'exige, l'entrepreneur /le sous-traitant étranger destinataire doit élaborer un formulaire de demande de consentement à utiliser lors de la cueillette de renseignements personnels ou un texte dans le cas de la cueillette de renseignements personnels par téléphone. L'entrepreneur/Le sous-traitant étranger destinataire ne peut utiliser le formulaire ou le texte sans avoir obtenu l'approbation écrite préalable de l'autorité contractante. Il doit aussi obtenir le consentement de l'autorité contractante avant de modifier le formulaire ou le texte.

(d) Si, lors de la cueillette de renseignements personnels auprès d'un individu, l'entrepreneur/le sous-traitant étranger destinataire sait ou soupçonne que cet individu n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, l'entrepreneur/le sous-traitant étranger destinataire doit demander des directives à l'autorité contractante.

15. Exactitude, confidentialité et intégrité des renseignements personnels

L'entrepreneur/Le sous-traitant étranger destinataire doit veiller à ce que les renseignements personnels soient les plus exacts, complets et à jour que possible. Pour ce faire, l'entrepreneur/le sous-traitant étranger destinataire doit, au minimum:

a) ne pas utiliser de données d'identification personnelle (par ex., le numéro d'assurance sociale, le numéro de passeport, le numéro d'identificateur client unique) pour lier de nombreuses bases de données qui comprennent des renseignements personnels;

b) isoler les dossiers des renseignements et des dossiers de **l'entrepreneur/du sous-traitant** étranger destinataire**;**

c) ne donner l'accès aux renseignements personnels et aux dossiers qu'à ceux qui le requièrent aux fins d'exécution des travaux (par exemple, en utilisant des mots de passe ou un accès biométrique);

d) donner de la formation à toute personne à laquelle **l'entrepreneur/le sous-traitant** étranger destinataire donne accès aux renseignements personnels concernant l'obligation d'assurer la confidentialité et de ne l'utiliser qu'aux fins d'exécution des travaux. **L'entrepreneur/Le sous-traitant** étranger destinataire doit donner cette formation avant d'autoriser l'accès aux renseignements personnels et préparer à cet effet un dossier accessible à l'autorité contractante, sur demande;

e) à la demande de l'autorité contractante, demander aux personnes ayant accès aux renseignements personnels de reconnaître, par écrit (sous une forme approuvée par l'autorité contractante), leurs responsabilités en matière de confidentialité des renseignements personnels, avant de leur en donner l'accès;

f) tenir un registre de toutes les demandes faites par un individu pour la révision de ses renseignements personnels et toutes les demandes de correction d'erreurs ou d'omissions concernant les renseignements personnels (que les demandes soient faites directement par un individu ou par le Canada au nom d'un individu);

g) joindre une note à tout dossier qu'un individu a demandé de corriger, mais que **l'entrepreneur/le sous-traitant** étranger destinataire a décidé, pour quelque raison que ce soit, de ne pas corriger. Lorsque cela se produit, l'entrepreneur doit immédiatement informer l'autorité contractante de la correction demandée et des raisons de **l'entrepreneur/le sous-traitant** étranger destinataire de ne pas l'effectuer. Si l'autorité contractante demande que la correction soit effectuée, **l'entrepreneur/le sous-traitant** étranger destinataire a l'obligation du faire;

h) tenir un registre de la date et de l'auteur de la dernière mise à jour de chaque dossier;

i) maintenir un journal de vérification électronique qui enregistre tous les accès et les tentatives d'accès des dossiers électroniques. Le journal de vérification doit être dans un format qui peut être lu par **l'entrepreneur/le sous-traitant** étranger destinataire et le Canada en tout temps;

j) sécuriser et contrôler l'accès à tout renseignement personnel.

16. Protection des renseignements personnels

L'entrepreneur/Le sous-traitant étranger destinataire doit protéger les renseignements personnels à tout moment en prenant toutes les mesures raisonnablement nécessaires pour les protéger et en protéger l'intégrité et la confidentialité. Pour ce faire, l'entrepreneur/le sous-traitant étranger destinataire doit au moins:

a) stocker les renseignements personnels sous format électronique de manière à ce qu'un mot de passe (ou un autre mécanisme de contrôle) soit requis pour accéder au système ou à la base de données où sont stockés les renseignements personnels;

b) s'assurer que les mots de passe ou autres moyens d'accès aux renseignements personnels ne sont fournis qu'aux individus qui le requièrent aux fins d'exécution des travaux;

c) ne pas confier à un tiers (y compris un affilié) le stockage des renseignements personnels sans l'autorisation préalable et écrite de l'autorité contractante;

d) protéger les bases de données ou les systèmes informatiques qui emmagasinent les renseignements personnels contre un accès externe de manière à protéger les renseignements très protégés et de nature délicate;

e) faire une sauvegarde et une mise à jour de tous les dossiers au moins une fois par semaine;

f) mettre en œuvre toutes les mesures de sécurité ou de protection demandées par le Canada de temps à autre;

g) aviser immédiatement l'autorité contractante de toute infraction (p. ex. un accès, un usage ou une divulgation non autorisé de renseignements) ou de tout incident pouvant mettre en danger la sécurité ou l'intégrité des dossiers, des systèmes ou des installations ou des renseignements personnels sont conservés. Si une infraction se produit, l'entrepreneur ou le sous-traitant devra immédiatement prendre toutes les mesures raisonnables nécessaires pour limiter l'étendue des impacts possibles ou pour résoudre le problème et empêcher celui-ci de se reproduire. Le Canada peut exiger de l'entrepreneur qu'il prenne des mesures précises pour régler le problème et éviter qu'il se reproduise, et pourrait invoquer les dispositions de la présente entente en lien avec la suspension ou la résiliation du contrat pour manquement.

17. Obligations réglementaires

a) L'entrepreneur/Le sous-traitant étranger destinataire reconnaît que le Canada est tenu de traiter tous les renseignements personnels et les dossiers conformément aux dispositions de la Loi sur la protection des renseignements personnels, de la Loi sur l'accès à l'information, L.R.C.1985, ch. A-1, et de la Loi sur la Bibliothèque et les Archives du Canada, L.C. 2004, ch.11. L'entrepreneur /Le sous-traitant étranger destinataire convient de se conformer aux exigences établies par l'autorité contractante qui sont requises pour permettre au Canada de remplir ses obligations en vertu de ces lois et toute autre loi qui entre en vigueur lorsqu'il y a lieu.

b) L'entrepreneur/Le sous-traitant étranger destinataire reconnaît que les obligations dont il doit s'acquitter en vertu du contrat s'ajoutent à toutes celles qui lui incombent en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques, L. C. 2000, ch.5, ou d'une loi similaire en vigueur dans une province ou un territoire du Canada. Si l'entrepreneur/le sous-traitant étranger destinataire estime que l'une ou l'autre des obligations du contrat l'empêche de s'acquitter de ses obligations en vertu de ces lois, il doit immédiatement informer l'autorité contractante de la disposition du contrat et de l'obligation de la loi qu'il considère comme contradictoires.

18. Obligation juridique de divulguer les renseignements personnels

a) Avant de divulguer tout renseignement personnel conformément à toute loi, à tout règlement ou toute ordonnance rendue par une cour de justice, un tribunal ou une entité administrative compétente, l'entrepreneur/le sous-traitant étranger destinataire doit immédiatement informer l'autorité contractante afin de lui permettre de participer aux procédures pertinentes.

19. Plaintes ou demandes d'accès

a) Le Canada et l'entrepreneur/le sous-traitant étranger destinataire conviennent de s'informer immédiatement et mutuellement de la réception d'une plainte en vertu de la Loi sur l'accès à l'information, de la Loi sur la protection des renseignements personnels ou de toute autre loi pertinente concernant les renseignements personnels. Les parties conviennent de s'échanger toute information nécessaire pour faciliter le règlement de la plainte et de s'informer immédiatement et mutuellement de son dénouement.

20. Exception

a) Les obligations énoncées dans ces articles ne s'appliquent pas aux renseignements personnels qui sont déjà du domaine public, du moment qu'elles ne sont pas devenues du domaine public, à la suite d'une faute ou d'une omission de l'entrepreneur/le sous-traitant étranger destinataire ou de tout sous-traitant, agent ou représentant de l'entrepreneur ou des employés.

Appendice D – Obligations en matière de sécurité

1. Généralités

(a) Objet

La présente appendice a pour objet d'énoncer les obligations du fournisseur en ce qui concerne la configuration et la gestion appropriées des actifs et des actifs informationnels, afin de protéger ces actifs et ces actifs contre toute modification, accès ou exfiltration non autorisés, le tout conformément au contrat, la présente appendice, les mesures de sécurité spécifiques du fournisseur et les politiques canadiennes en matière de sécurité et de confidentialité (collectivement appelées «obligations de sécurité et de confidentialité»).

(b) Exécution des obligations en matière de protection de la vie privée

Les obligations du fournisseur contenues dans les présentes obligations de sécurité et confidentialité doivent être transférées par le fournisseur aux sous-processeurs du fournisseur, dans la mesure où elles s'appliquent à chaque sous-processeur du fournisseur, étant donné la nature des services fournis au fournisseur.

(c) Gestion du changement

Le fournisseur doit, pendant toute la durée du contrat, prendre toutes les mesures nécessaires pour mettre à jour et maintenir à jour les obligations en matière de sécurité et de confidentialité afin de se conformer aux pratiques de sécurité des normes de l'industrie.

Le fournisseur doit accepter d'informer le Canada de toutes les améliorations qui pourraient avoir une incidence sur les services dans le contrat, y compris les améliorations techniques, administratives ou tout autre type d'améliorations. Le fournisseur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier, sans supplément pour le Canada.

2. Reconnaissance

Les parties reconnaissent que:

a) Tous les biens et les actifs informationnels sont assujettis à ces obligations en matière de sécurité et de confidentialité.

b) Nonobstant toute autre disposition de la présente appendice, les parties partagent la responsabilité d'élaboration et du maintien des politiques, des procédures et des contrôles de sécurité relatifs aux biens et aux actifs informationnels.

c) Le fournisseur ne doit pas avoir ou tenter d'obtenir la garde d'un actif d'information, ni permettre à un membre du personnel des services à accéder à un actif information avant la mise en œuvre des obligations de sécurité et de confidentialité requises, comme l'exige la présente appendice, au plus tard à l'attribution du marché.

d) Les obligations de sécurité s'appliquent au Palier 1 (jusqu'à la protection A / blessures faibles) et au Palier 2 (jusqu'à la protection B / blessures moyennes), sauf indication contraire.

3. Sécurisation des actifs informatiques

a) Les solutions logiciels-services du fournisseur doivent être conçues de manière à protéger les actifs et les actifs informatiques contre tout accès, modification ou exfiltration non autorisés. Cela inclut la mise en œuvre et la maintenance de stratégies, procédures et contrôles de sécurité des informations appropriés pour préserver la confidentialité, l'intégrité et la disponibilité des actifs et des actifs informatiques (ci-après dénommés les «mesures de sécurité spécifiques»).

4. Roles and Responsibilities for Security

(a) Le fournisseur doit définir clairement les rôles et les responsabilités en ce qui concerne les contrôles de sécurité les fonctionnalités des services entre le fournisseur (tout sous-processeur du fournisseur, le cas échéant) et le Canada. 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.

(b) Le fournisseur doit fournir au Canada un document à jour qui définit les rôles et les responsabilités du fournisseur, des sous-traitants du fournisseur et du Canada en matière de contrôles et de caractéristiques de sécurité : (i) sur une base annuelle; (ii) lorsqu'il y a des changements importants à ces rôles et responsabilités à la suite d'un changement aux services; ou (iii) à la demande du Canada.

5. Assurance de partie tierce: certifications et rapports

(a) Le fournisseur doit s'assurer que tous les actifs, l'infrastructure du fournisseur (y compris tout service IaaS, PaaS ou SaaS fourni au Canada) et les emplacements de service sont sécurisés conformément aux certifications de l'industrie et aux rapports d'audit.

(b) Le fournisseur doit démontrer sa conformité aux certifications et rapports d'audit suivants en fournissant des rapports d'évaluation ou des certifications de tiers indépendants pour TOUTES les parties du service:

(i) ISO / CEI 27001: 2013 Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Certification obtenue par un organisme de certification accrédité; OU

(ii) AICPA Service Organization Control (SOC) 2 Rapport d'audit de type II 2 Type II pour les principes de confiance de la sécurité, de la disponibilité, de l'intégrité du traitement et de la confidentialité - délivré par un expert-comptable agréé indépendant; Et

(iii) Auto-évaluation de ses services par rapport à Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 ou version ultérieure.

(c) Le fournisseur doit démontrer la conformité aux certifications et rapports d'audit suivants en fournissant des rapports d'évaluation ou des certifications de tiers indépendants pour TOUTES les parties du service:

(i) ISO / CEI 27001: 2013 Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Certification obtenue par un organisme de certification accrédité; ET

(ii) ISO / CEI 27017: 2015 Technologies de l'information - Techniques de sécurité - Code de pratique pour les contrôles de sécurité de l'information basé sur ISO / CEI 27002 pour les services de cloud computing réalisé par un organisme de certification accrédité; ET

(iii) AICPA Service Organisation Control (SOC) 2 Rapport d'audit de type II 2 Type II pour les principes de confiance de la sécurité, la disponibilité, l'intégrité du traitement et la confidentialité - délivré par un expert-comptable agréé indépendant.

(d) Le fournisseur doit démontrer la conformité à ces certifications et rapports d'audit en fournissant des rapports d'évaluation indépendants ou des certifications pour toutes les parties du service.

(e) Chaque rapport de certification ou d'audit fourni doit: (i) identifier le nom commercial légal du fournisseur ou du sous-traitant fournisseur applicable; (ii) identifier la date de certification du fournisseur ou du sous-traitant fournisseur et le statut de cette certification; (iii) identifier la liste des actifs, de l'infrastructure des fournisseurs et des emplacements de service dans le cadre du rapport de certification. Si la méthode spécifiée est utilisée pour exclure les organisations de sous-service telles que l'hébergement de centre de données, le rapport d'évaluation de l'organisation de sous-service doit être inclus.

(f) Chaque certification ISO fournie doit être valable pendant toute la durée du contrat, dans les 12 mois précédant le début du contrat. Les certifications doivent être accompagnées de pièces justificatives telles que le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO.

(g) Chaque rapport d'audit SOC doit avoir été réalisé dans les 12 mois précédant le début du contrat.

(h) Le fournisseur doit maintenir la devise de sa certification selon les normes décrites au paragraphe 5 (1) tout au long du contrat. Le fournisseur doit fournir, au moins une fois par an et rapidement à la demande du Canada, tous les rapports ou dossiers qui peuvent être raisonnablement requis pour démontrer que les certifications du fournisseur restent à jour et sont valables pour la durée du contrat.

6. Vérification de la conformité aux obligations de sécurité

(a) Le fournisseur doit effectuer les vérifications de confidentialité et de sécurité, de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter et protéger les biens et les actifs d'information, comme suit :

(i) Lorsqu'une norme ou un cadre prévoit des vérifications, une vérification de cette norme ou de ce cadre de contrôle sera entreprise au moins une fois par année;

(ii) Chaque vérification sera effectuée conformément aux normes et aux règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable; et

(iii) Chaque vérification sera effectuée par un vérificateur tiers qualifié et indépendant qui (i) est qualifié selon l'AICPA, CPA Canada ou le régime de certification ISO, et (ii) se conforme à la norme ISO/IEC 17 020 sur les systèmes de management de la qualité à la sélection et aux frais du fournisseur.

b. Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être communiqué au Canada. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le vérificateur externe. Le fournisseur doit corriger rapidement et à la satisfaction du vérificateur les problèmes soulevés dans tout rapport de vérification et doit (i) fournir au Canada le plan pour corriger toute constatation négative découlant de ces rapports et (ii) fournir au Canada, sur demande, des rapports d'étape sur la mise en œuvre dans les dix (10) jours ouvrables du gouvernement fédéral.

7. Programme d'évaluation de sécurité de la TI

(a) En plus des certifications de l'industrie décrites à la section 5 (assurance tierce partie: certifications et rapports), le fournisseur doit démontrer la conformité aux exigences de sécurité sélectionnées dans le profil de contrôle de sécurité du GC pour les services informatiques du GC disponibles dans le cloud (https : //www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) ou version ultérieure, pour l'étendue des Services fournis par le Fournisseur. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications applicables de l'industrie identifiées ci-dessous, et validée par des évaluations indépendantes par des tiers.

(b) La conformité sera validée et vérifiée par le biais du processus d'évaluation de la sécurité des technologies de l'information (TI) du fournisseur de services en nuage (CSP) du Centre canadien pour la cybersécurité (CCCS) (ITSM.50.100) (https://cyber.gc.ca/fr / guidance / cloud-service-provider-information-technology-security-assessment-process-itsm50100).

(i) Tout fournisseur qui a participé au processus doit fournir des documents confirmant qu'il a terminé le processus d'intégration avec (i) une copie du plus récent rapport d'évaluation complété fourni par le CCCS; et (ii) une copie du rapport de synthèse le plus récent fourni par le CCCS.

(ii) Pour lancer le processus d'intégration, le fournisseur doit contacter les services à la clientèle du CCCS pour recevoir une copie du formulaire de soumission d'intégration et toute information supplémentaire relative au programme d'évaluation informatique du CSP.

(c) À la demande du Canada, des preuves supplémentaires du fournisseur, y compris des plans de sécurité du système, des conceptions ou des documents d'architecture qui fournissent une description complète du système, peuvent être fournies par le fournisseur ou un sous-traitant fournisseur pour compléter la certification et l'audit. les rapports décrits à la section 5 (assurance de tiers) afin de démontrer la conformité du fournisseur avec les certifications requises de l'industrie.

8. Protection des données

(a) Le fournisseur doit:

(i) Mettre en œuvre le chiffrement des données au repos pour tous les actifs informationnels.

(ii) (ii) Prendre des mesures raisonnables pour garantir que le chiffrement des données au repos reste en vigueur, ininterrompu et actif à tout moment, même en cas de défaillance de l'équipement ou de la technologie.

(iii) (iii) Transmettre les actifs informationnels de manière sécurisée. Cela comprend la mise en œuvre du chiffrement des données en transit pour toutes les transmissions d'actifs et d'actifs d'information.

(iv) (0iv) Mettre en œuvre des contrôles de sécurité qui restreignent l'accès administratif aux actifs et systèmes d'information par le fournisseur et permettent de demander l'approbation du Canada avant que le fournisseur puisse accéder aux actifs d'information pour effectuer des activités de soutien, de maintenance ou opérationnelles à l'aide des actifs d'information constitués du Canada Les données.

(v) (v) Prendre des mesures raisonnables pour s'assurer que le personnel des services n'a pas de droits d'accès permanents ou continus aux actifs informationnels, et l'accès est limité à ceux qui doivent accéder aux actifs et actifs informationnels pour fournir un soutien technique ou à la clientèle en fonction de l'approbation du Canada.

(b) Le fournisseur ne doit faire aucune copie des bases de données ou toute partie de ces bases de données contenant des actifs informationnels, et ne doit pas déplacer ou transmettre des copies approuvées à quelque endroit que ce soit, sauf si l'approbation est obtenue du Canada.

9. **Isolement des données**

Le fournisseur doit mettre en œuvre des contrôles pour garantir une isolation appropriée des ressources de sorte que les actifs informationnels ne soient pas mélangés avec d'autres données de locataires, pendant leur utilisation, leur stockage ou leur transit, et dans tous les aspects des fonctionnalités du service du fournisseur et de l'infrastructure du fournisseur et de l'administration du système. Cela inclut la mise en œuvre de contrôles d'accès et l'application d'une ségrégation logique ou physique appropriée pour prendre en charge:

(a) La séparation entre l'administration interne du Fournisseur et les ressources utilisées par ses clients; et

(b) (b) La séparation des ressources client dans les environnements multi-locataires afin d'empêcher un consommateur malveillant ou compromis d'affecter le service ou les données d'un autre.

10. Emplacement des données

(a) Le fournisseur doit avoir la capacité pour le Canada de stocker et de protéger ses actifs d'information, au repos, y compris les données dans des sauvegardes ou conservées à des fins de redondance. Cela comprend la possibilité d'isoler des données au Canada dans des centres de données approuvés. Un centre de données approuvé est défini comme suit:

(i) Un centre de données qui répond à toutes les exigences et certifications de sécurité identifiées à la section 33 pour la sécurité physique (centre de données / installations)

(ii) garantit l'impossibilité de trouver les données d'un client spécifique sur des supports physiques; et

(b) Utilise le cryptage pour garantir qu'aucune donnée n'est écrite sur le disque sous une forme non cryptée.

(c) Le fournisseur doit certifier que la livraison et la fourniture de services dans le cadre de ce contrat proviennent de pays de l'Organisation du Traité de l'Atlantique Nord (OTAN) (https://www.nato.int/cps/en/natohq/nato_countries.htm) ou l'Union européenne (UE) (https://europa.eu/european-union/about-eu/countries_en), ou de pays avec lesquels le Canada a un instrument international bilatéral de sécurité industrielle. Le programme de sécurité des contrats (PSC) comprend des instruments internationaux bilatéraux de sécurité industrielle avec les pays répertoriés sur le site Web de SPAC suivant: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html et mis à jour à partir de de temps en temps.

(d) Le fournisseur doit avoir la capacité pour le Canada d'isoler les actifs et les actifs informationnels dans les centres de données qui sont géographiquement situés au Canada.

(e) Sur demande, le fournisseur doit:

(i) Fournir au GC une liste à jour des emplacements physiques, y compris la ville, qui peuvent contenir des actifs et des actifs d'information pour chaque centre de données qui seront utilisés pour fournir des services; et

(ii) Identifier les parties des Services qui sont livrées de l'extérieur du Canada, y compris tous les emplacements où les données sont stockées et traitées et d'où le Fournisseur gère le service.

(f) Le fournisseur des services proposés a l'obligation continue d'aviser le Canada lorsqu'il y a des mises à jour de la liste des emplacements physiques pouvant contenir des actifs et des actifs informationnels.

11. Transfert et récupération des données

Le fournisseur doit, à la demande du Canada :

(a) Extraire tous les fichiers en ligne, pseudo-direct et hors ligne;

(b) Transfert sécurisé de tous les actifs d'information, y compris les métadonnées, dans un format lisible et utilisable par machine acceptable pour le Canada, conformément aux Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires à valeur continue de Bibliothèque et Archives Canada (https://www.bac-lac.gc.ca/fra/services/gestion-ressources-documentaires-gouvernement/lignes-directrices/Pages/lignes-directrices-formats-fichier-transferers-ressources-documentaires.aspx).

12. Disposition des dossiers et remise des dossiers au Canada

(a) Le fournisseur (palier 1 et 2) doit, sur demande, éliminer ou réutiliser en toute sécurité les ressources (p. ex. l'équipement, le stockage des données, les fichiers et la mémoire) qui contiennent des actifs d'information et s'assurer que les données précédemment stockées ne peuvent être traitées par d'autres clients après leur diffusion. Cela touche toutes les copies des actifs d'information qui sont créées aux fins de disponibilité accrue et de reprise après sinistre. L'élimination ou la réutilisation des ressources par le fournisseur doit être harmonisée à l'un des documents suivants : (i) Manuel d'utilisation du Programme national de sécurité industrielle (DoD 5220.22-M6); (ii) Lignes directrices pour l'assainissement des supports (NIST SP 800-88); ou (iii) Effacement et déclassification des supports d'information électroniques (CSTC ITSG-06).

(b) Le fournisseur doit fournir des preuves démontrant qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de tout système, de toute capacité (logiciel ou processus), de toute donnée ou de toute information retirés ou détruits après leur retrait de l'instance du Canada.

13. Protection Cryptographique

Le fournisseur doit:

(a) 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;

(b) 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);

(c) 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

(d) 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

14. Gestion des clés

Le fournisseur doit posséder la capacité de fournir au Canada un service de gestion de clés qui permet :

a) la création/génération et la suppression des clés utilisées pour livrer la Solution SaaS de cryptage par le GC;

b) la définition et l'application de politiques propres au gouvernement du Canada qui contrôlent la façon dont les clés peuvent être utilisées;

c) la protection de l'accès au matériel clé, y compris la prévention de l'accès du fournisseur au matériel clé de façon non chiffrée; et

d) la vérification de tous les événements liés aux principaux services de gestion, y compris l'accès des fournisseurs aux fins d'examen par le Canada.

15. Contrôle d'accès

Le fournisseur doit avoir la capacité pour le Canada de prendre en charge un accès sécurisé aux services, y compris la capacité de configurer:

(a) authentification multifactorielle conformément à l'ITSP.30.031 V2 du CST (ou versions ultérieures) (https://www.cse-cst.gc.ca/en/node/1842/html/26717) à l'aide de justificatifs d'identité approuvés par le GC ;

(b) accès basé sur les rôles;

(c) Contrôle d'accès aux objets stockés; et

(d) Politiques d'autorisation granulaires pour autoriser ou limiter l'accès.

16. Gestion d'accès privilégié

Le fournisseur doit fournir une documentation démontrant comment le logiciel en tant que service est en mesure de répondre aux exigences de sécurité suivantes:

(a) gérer et surveiller l'accès privilégié aux services cloud pour garantir que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles utilisées pour héberger les services du GC;

(b) restreindre et minimiser l'accès aux services et aux ressources d'information du Canada uniquement aux appareils autorisés et aux utilisateurs finaux ayant un besoin explicite d'y avoir accès;

(c) faire respecter et vérifier les autorisations d'accès aux services et aux actifs informationnels;

(d) restreindre tout accès aux interfaces de service qui hébergent des actifs et des actifs d'information à des utilisateurs finaux, des dispositifs et des processus (ou services) identifiés, authentifiés et autorisés de manière unique;

(e) Mettre en œuvre des politiques de mot de passe pour protéger les informations d'identification contre toute compromission par des attaques en ligne ou hors ligne et pour détecter ces attaques en enregistrant et en surveillant les événements tels que (i) l'utilisation réussie des informations d'identification, (ii) l'utilisation inhabituelle des informations d'identification, et (iii) l'accès et l'exfiltration à partir de la base de données de mots de passe, conformément à ITSP.30.031 V2 du CST (ou versions ultérieures) (https://www.cse-cst.gc.ca/en/node/1842/html/26717) ;

(f) Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux avec un accès privilégié, conformément à ITSP.30.031 V2 du CST (ou versions ultérieures) (https://www.cse-cst.gc.ca/en/node/1842 / html / 26717);

g) Mettre en œuvre des mécanismes de contrôle d'accès basés sur les rôles pour attribuer des privilèges qui constituent la base pour imposer l'accès aux actifs et aux actifs informationnels;

h) Définir et mettre en œuvre la séparation des tâches pour réaliser, au minimum, la séparation des rôles de gestion et d'administration des services des rôles de soutien du système d'information, des rôles de développement des rôles opérationnels et des rôles de gestion des accès des autres rôles opérationnels;

(i) Adhérer aux principes de moindre privilège et de besoin de savoir lors de l'octroi de l'accès aux Services et Actifs et aux Actifs d'Information;

(j) Utiliser des points de terminaison sécurisés (par exemple, des ordinateurs, des appareils d'utilisateur final, des serveurs de saut, etc.) qui sont configurés pour la moindre fonctionnalité (par exemple, un point de terminaison dédié qui n'a pas de navigation sur Internet ou d'accès ouvert au courrier électronique) pour fournir un soutien et une administration des services et de l'infrastructure des fournisseurs;

(k) Mettre en œuvre un processus automatisé pour auditer périodiquement, au minimum, les actions de création, modification, activation, désactivation et suppression de compte; et

(l) En cas de cessation d'emploi, résiliez ou révoquez les authentifiant et les identifiants d'accès associés à tout personnel des services.

17. Gestion des comptes de base/principal

Le fournisseur doit assurer la protection adéquate du processus de gestion des comptes et de gestion des factures utilisé pour établir les mesures de sécurité, notamment:

(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) Assurer la séparation des fonctions des individus;

(c) Utiliser le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés;

(d) Veiller à ce que les utilisateurs autorisés reçoivent une sensibilisation à la sécurité et une formation dans le cadre de l'emploi à bord et lorsque leur rôle change et soient informés des exigences de sécurité associées au contrat.

(e) créer, protéger et conserver les dossiers d'audit liés aux activités qui soutiennent la gestion des comptes des services fournis au Canada;

(f) fournir au Canada des rapports sur les événements vérifiés pour les mesures liées à l'émission et à la gestion des comptes principaux utilisés par le personnel pour gérer les comptes du GC;

(g) Mettre en œuvre des mesures de sécurité qui accordent et maintiennent le niveau requis de filtrage de sécurité pour le personnel chargé de la gestion des comptes principaux liés au Canada, conformément à la LVERS; et

(h) Veiller à ce que les actifs et les actifs informationnels soient protégés pendant et après les actions du personnel telles que les licenciements et les transferts. Assurer la séparation des tâches des individus.

18. Fédération

Le fournisseur doit permettre au Canada de soutenir l'intégration de l'identité fédérée, notamment:

(a) Prise en charge du langage SAML (Security Assertion Markup Language) 2.0 et d'OpenID Connect 1.0, où les informations d'identification de l'utilisateur final et l'authentification aux services nuagiques sont sous le contrôle exclusif du Canada; et

(b) Capacité d'associer des identifiants uniques au Canada (par exemple, un identifiant unique au Canada, une adresse électronique au Canada, etc.) avec le ou les comptes d'utilisateur du service cloud correspondants.

19. Protection des terminaux

(a) Le fournisseur doit mettre en œuvre, gérer et surveiller les points de terminaison sécurisés pour éviter les attaques et les utilisations abusives conformément aux directives de configuration reconnues par l'industrie telles que celles figurant dans NIST 800-123 (Guide to General

Server Security), le Center for Internet (CIS) Repères ou norme équivalente approuvée par écrit par le Canada.

20. Développement sécurisé

(a) 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 du cycle de vie du système d'information et dans le développement de logiciels, de sites Web et de services, et se conforme aux normes et meilleures pratiques de l'industrie, telles que (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode, ou (v) les normes Open Web Application Security Project (OWASP) telles que Application Security Verification Standard (ASVS) ou une norme équivalente approuvée par le Canada en l'écriture.

21. Interface de programmation d'application (API)

Le fournisseur doit:

a) Fournir des services qui utilisent des interfaces de programmation d'applications (API) ouvertes, publiées, prises en charge et documentées, afin de prendre en charge l'interopérabilité entre les composants et de faciliter la migration des applications.

b) Prendre des mesures raisonnables pour protéger les API internes et externes au moyen de méthodes d'authentification sécurisées. Cela implique de s'assurer que toutes les requêtes d'API exposées en externe nécessitent une authentification réussie avant de pouvoir être appelées.

c) Pour la solution logiciel-service, le fournisseur doit fournir des API qui permettent:

(i) d'interroger des données inactives dans des applications de la solution logiciel-service; et

(ii) d'évaluer les événements et les incidents stockés dans les journaux d'applications de la solution logiciel-service.

22. Sécurité des réseaux et des communications

Le fournisseur doit :

a) Permettre au Canada d'établir des connexions sécurisées aux Services, notamment en assurant la protection des données en transit entre le Canada et le Service au moyen de TLS 1.2 ou de versions ultérieures, et en utilisant des algorithmes et des certificats cryptographiques pris en charge, comme le décrit les normes ITSP.40.062 (https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles- reseFournit une protection des données en transit entre les microservices et les au-itsp40062) et ITSP.40.111 (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b) du CST; applications utilisées au sein des Services;

b) Utiliser des certificats correctement configurés dans les connexions TLS conformément aux directives du CST.

c) Désactiver les protocoles vulnérables connus, comme toutes les versions de Secure Sockets Layer (SSL) (p. ex. SSLv2 et SSLv3) et toutes les versions antérieures de TLS (p. ex. TLS 1.0 et TLS 1.1), conformément à la norme ITSP.40.062 du CST, ainsi que les modes de chiffrement vulnérables connus (p. ex. RC4 et 3DES); et

d) Permettre au Canada de mettre en œuvre des contrôles d'accès au réseau et des règles de sécurité qui permettent ou refusent le trafic réseau vers les ressources canadiennes.

23. Connexions dédiées

L'entrepreneur doit permettre au GC d'établir une connectivité privée redondante aux services. Cela comprend :

a) Établir une connectivité soit directement dans le réseau étendu du GC (WAN), soit via le fournisseur d'échange de cloud GC situé au 151 Front à Toronto et / ou au 625 René Levesque à Montréal;

b) Activation de services complets de sauvegarde et de reprise après sinistre grâce à des connexions redondantes au sein et entre les centres de données de l'entrepreneur;

c) des liaisons de connectivité physique qui sont optiques et qui offrent un minimum de 10 Gbit / s avec la possibilité de regrouper des liaisons 10 G supplémentaires jusqu'à 40 G, avec une connectivité 100 G en option;

d) la prise en charge de la virtualisation et de locataires multiples pour tous les composants réseau;

e) la prise en charge de protocoles de routage dynamiques (Border Gateway Protocol) pour toutes les connexions;

f) la prise en charge de protocoles approuvés par le GC, qui sont décrits dans les documents suivants :

(i) Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062), Section 3.1 (suites de chiffrement AES)
(ii) Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)

g) Fournir une description des emplacements géographiques de tous les centres de données au Canada où cette capacité est offerte.

24. **Journalisation et vérification**

a) des contrôles de production et de gestion de journaux pour toutes les composantes du service qui stockent ou traitent les biens et les actifs d'information, et qui sont conformes aux pratiques des principaux fournisseurs de services, comme celles de NIST 800-92 (Guide to Computer Security Log Management), ou une norme équivalente approuvée par écrit par le Canada.

b) Le fournisseur doit permettre au Canada d'examiner et d'analyser de manière centralisée les dossiers de vérification de multiples composants des services offerts par le fournisseur. Ceci comprend la capacité pour le Canada :

(i) d'enregistrer et de détecter les événements de vérification tels qu'un minimum (i) de tentatives de connexion réussies ou non, (ii) de gestion des comptes, (iii) d'accès aux objets et changement de politique, (iv) de fonctions de privilèges et de suivi des processus, (v) d'événements système, (vi) de suppression des données;

(ii) d'enregistrer dans des journaux (ou fichiers journaux) des événements de vérification qui sont synchronisés et horodatés en temps universel coordonné (UTC) et protégés contre l'accès, la modification ou la suppression non autorisé pendant le transport et au repos;

(iii) des incidents de sécurité et des journaux de bord distincts pour les différents comptes du Canada afin de permettre au Canada de surveiller et de gérer les événements à l'intérieur de ses frontières qui ont une incidence sur l'instance d'un service IaaS, PaaS ou SaaS qui lui est fourni par le fournisseur ou un sous-traitant du fournisseur; et

(iv) de transmettre les événements et journaux des locataires du Canada vers un système centralisé de journaux de vérification géré par le gouvernement au moyen d'interfaces d'établissement Format [CEF], Syslog et autres formats communs) et d'interface de programmation d'application normalisés qui permettent la récupération à distance des données de journaux (par l'intermédiaire d'une interface de base de données qui utilise SQL, etc.).

25. Surveillance continue

a) Le fournisseur doit continuellement gérer, surveiller et maintenir la posture de sécurité de tous les biens, de l'infrastructure du fournisseur et des emplacements de service pendant toute la durée du contrat, et s'assurer que les services fournis au Canada sont conformes aux présentes obligations en matière de sécurité. Dans le cadre de l'obligation, l'entrepreneur doit :

(i) surveiller activement et continuellement les menaces et les vulnérabilités pesant sur les actifs, l'infrastructure du fournisseur, les emplacements de service ou les actifs d'information;

(ii) faire de son mieux pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le refus de service;

(iii) faire de son mieux pour détecter les attaques, les incidents de sécurité et autres événements anormaux;

(iv) détecter l'utilisation et l'accès non autorisés à tous les services, données et composants pertinents aux services IaaS, PaaS ou SaaS du Canada;

(v) gérer et appliquer les correctifs et les mises à jour liés à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de remédier à tout problème signalé publiquement dans les services ou les bibliothèques que les services utilisent, et fournir des avis préalables liés aux correctifs conformément aux engagements convenus relatifs au niveau de service;

(vi) répondre aux menaces et aux attaques contre les services du fournisseur, les contenir et veiller à la récupération;

(vii) au besoin, prendre des contre-mesures proactives, y compris, des mesures préventives et d'intervention permettant d'atténuer les menaces.

b) Les services de l'entrepreneur doivent permettre de copier les données des applications (IaaS, PaaS et SaaS) et le trafic réseau (IaaS et PaaS) du gouvernement du Canada dans les services infonuagiques hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du gouvernement).

c) Les services de l'entrepreneur doivent permettre au Canada de déployer et d'utiliser des logiciels de sécurité pour assurer la surveillance avancée et l'atténuation des cyber-menaces pour les services du Canada à l'échelle de l'hôte géré par le gouvernement et de la couche réseau, pour les composants gérés par le Canada seulement.

26. Notifications

Le fournisseur doit fournir :

a) Une notification rapide de toute interruption qui peut avoir une incidence sur la disponibilité et le rendement du service (comme convenu entre les parties et indiqué dans l'énoncé de travail ou l'entente sur les niveaux de service [ENS]);

b) Des bilans réguliers au sujet des procédures de restauration des services à un état opérationnel selon les ENS et les exigences en matière de disponibilité du système convenues, sous forme d'alertes transmises avant et après la mise en œuvre;

c) Des alertes, des avis et des directives de sécurité liés au système d'information, par courriel, pour les vulnérabilités qui constituent une menace pour les services.

27. Gestion des incidents de sécurité

a) Le processus d'intervention en cas d'incident de sécurité du fournisseur pour les services doit englober les pratiques du cycle de vie de la gestion des incidents de sécurité informatique et les pratiques d'appui des activités de préparation, de détection, d'analyse, de confinement et de récupération, conformément à l'une des normes suivantes : (i) ISO/IEC 27035:2011 Technologies de l'information -- Techniques de sécurité --

Management des incidents liés à la sécurité de l'information; ou (ii) NIST SP800-612, Computer Security Incident Handling Guide; ou (iii) Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGECGC)
[https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html];
ou (iv) autres pratiques exemplaires des principaux fournisseurs de services si le Canada détermine, à sa discrétion, que celles-ci respectent ses exigences en matière de sécurité.

b) Le processus d'intervention en cas d'incident de sécurité du fournisseur doit comprendre ce qui suit :

(i) des processus et procédures documentés indiquant comment le fournisseur relèvera les incidents de sécurité, y donnera suite et y remédiera, dressera un rapport à leur sujet et les signalera au Canada, y compris : (i) la portée des incidents de sécurité que le fournisseur doit signaler au Canada; (ii) le degré de divulgation et les mesures utilisées par le fournisseur pour détecter les incidents de sécurité, ainsi que les interventions connexes du fournisseur pour des types précis d'incidents de sécurité; (iii) le délai cible de signalement et de transmission des incidents de sécurité; (iv) la procédure de signalement et d'acheminement en cas d'incidents de sécurité; (v) les coordonnées des personnes-ressources pour le traitement des enjeux relatifs aux incidents de sécurité; (vi) tout recours applicable à certains incidents de sécurité.

(ii) des procédures pour répondre aux demandes de preuve numérique potentielle ou d'autres renseignements provenant de l'environnement de service ou de l'infrastructure du fournisseur, y compris les procédures judiciaires et les mesures de protection pour la tenue d'une chaîne de possession des actifs d'information stockés ou traités par le fournisseur ou un sous-traitant du fournisseur. Les pratiques et les contrôles en matière d'éléments de preuve judiciaires et numériques doivent être conformes aux pratiques des principaux fournisseurs de services, comme celles décrites dans la norme NIST 800-62 (Guide to Integrating Forensic Techniques into Incident Response), la norme ISO 27037 (Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuve numérique), ou une norme équivalente approuvée par écrit par le Canada.

28. Intervention en cas d'incident de sécurité

a) Si le fournisseur prend connaissance d'une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée des données ou l'accès accidentel ou illégal aux données du client ou des données personnelles du client pendant le traitement par le fournisseur (chacun étant un « incident de sécurité »), le fournisseur doit rapidement et sans tarder (i) informer le Canada de cet incident de sécurité; (ii) mener une enquête et fournir des renseignements détaillés sur cet incident de sécurité; (iii) prendre les mesures raisonnables pour atténuer les effets et les dommages découlant de l'incident de sécurité.

b) Le fournisseur doit alerter et aviser promptement le Canada (par téléphone et par courriel) de toute compromission, de toute violation ou de toute preuve comme (i) un incident de sécurité, (ii) une défectuosité liée à la sécurité d'un actif, (iii) l'accès irrégulier ou non autorisé à un actif, (iv) la copie à grande échelle d'un actif d'information ou (v) toute autre activité illégale recensée par le fournisseur, portant ce dernier à croire de manière raisonnable que le risque de compromission, d'atteinte à la sécurité ou à la vie privée est ou pourrait être imminent, ou si les mesures de protection existantes ont cessé de fonctionner, au cours de la période suivante (tous les jours, 24 heures par jour, 365 jours par année), et sans tarder, dans tous les cas, dans les 24 heures.

c) Le fournisseur doit collaborer avec le Canada au confinement, à l'éradication et à la récupération des incidents de sécurité conformément au processus d'intervention en cas d'incident de sécurité du fournisseur et au Plan de gestion des événements de cybersécurité du gouvernement du Canada

(PGECGC) (https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html). Notamment :

(i) ne permettre qu'aux représentants désignés du Canada :

1. de demander et de recevoir des renseignements liés à l'incident de sécurité et à tout actif d'information compromis (y compris, données des utilisateurs, journaux d'événements du système et de sécurité, saisies de paquets du réseau ou de l'hôte, journaux de composants de sécurité comme des systèmes de détection et de prévention d'intrusion et des pare-feux, etc.), dans un format non chiffré, à des fins de réalisation d'enquêtes;

2. d'assurer le suivi de l'état d'un événement signalé lié à la sécurité de l'information ou d'un incident de sécurité.

(ii) d'appuyer les efforts d'enquête du Canada dans le cas de toute compromission des utilisateurs ou des données du service relevé.

Le fournisseur doit de plus :

a) tenir un registre des violations de la sécurité comprenant une description de la violation de la sécurité, la durée, les conséquences de la violation, le nom de la personne ayant signalé la violation, et la personne à qui la violation a été signalée, et la procédure pour récupérer les données ou le service;

b) assurer le suivi ou permettre au Canada d'assurer le suivi des divulgations d'actifs et de renseignements, y compris les données qui ont été divulguées, à qui, et à quel moment.

29. Découverte électronique et blocages juridiques

a) Le fournisseur doit (et doit, dans la mesure où cela est applicable compte tenu de la nature des services sous-traités fournis par chaque sous-traitant fournisseur, exiger des sous-traitants fournisseurs) qu'il prenne des mesures raisonnables pour garantir que les services fournissent une découverte électronique et une prise légale. des fonctions pour les journaux des événements de sécurité afin de permettre au Canada de mener des enquêtes de sécurité en temps opportun et efficaces et de répondre aux demandes judiciaires de suspension judiciaire.

30. Test de pénétration

a) Le fournisseur doit avoir un processus qui permet au Canada d'effectuer une analyse de vulnérabilité ou un test de pénétration non perturbateur et non destructif de la partie canadienne des composants du service dans l'environnement du fournisseur.

31. Sécurité du personnel

a) (a) Le fournisseur doit (et doit, dans la mesure où cela est applicable compte tenu de la nature des services sous-traités fournis par chaque sous-traitant fournisseur, exiger des sous-traitants fournisseurs):

(i) Entreprendre une vérification de la diligence raisonnable des employés pour tout le personnel des services avant de recevoir l'autorisation d'accéder aux systèmes des fournisseurs ou aux ressources d'information; et

(ii) Mettre en œuvre des mesures de sécurité qui accordent et maintiennent le niveau requis de filtrage de sécurité pour le personnel des services conformément à leurs privilèges d'accès aux systèmes sur lesquels les actifs informationnels sont stockés et traités.

b) Les mesures en matière de filtrage de sécurité seront 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 à une norme équivalente approuvée par le Canada. Cette description doit inclure, à tout le moins, les éléments qui suivent :

(i) 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;

(ii) 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;

(iii) Le processus relatif à la sensibilisation et à la formation en matière de sécurité dans le cadre de l'intégration à l'emploi et lorsque les rôles des employés et des sous-traitants changent;

(iv) Le processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi; et

(v) Approche de détection des initiés malveillants potentiels et des contrôles mis en œuvre pour atténuer le risque d'accès aux données du GC ou d'incidence sur la fiabilité du logiciel-service hébergeant les actifs et les données du gouvernement du Canada.

32. Sécurité physique des installations des centres de données

Le fournisseur du logiciel-service public commercial proposé doit mettre 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 gouvernement du Canada sont stockées et protégées contre toute forme de manipulation, de perte, de dommages et de saisie, et qui sont fondées sur une approche de détection et de récupération préventive en matière de sécurité physique.

Cette description doit inclure, à tout le moins, les éléments qui suivent :

(a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont 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;

(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 autorises et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, et valider l'accès au moyen de deux formes d'identification;

(f) l'accompagnement des visiteurs et la surveillance de leur activité;

(g) la tenue des 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 à d'autres lieux de travail (p. ex., les sites de télétravail); et

33. Gestion des risques de la chaîne d'approvisionnement

(a) Le fournisseur des services doit mettre en œuvre des mesures de protection pour atténuer les menaces et les vulnérabilités de la chaîne d'approvisionnement des services informatiques afin de maintenir la confiance dans la sécurité des sources des systèmes d'information et des composants informatiques utilisés pour fournir les services. Cela comprend, mais sans s'y limiter, la conception et la mise en œuvre de contrôles pour atténuer et contenir les risques de sécurité des données grâce à une séparation appropriée des tâches, un accès basé sur les rôles et un accès au moindre privilège pour tout le personnel de la chaîne d'approvisionnement.

(b) Le fournisseur doit fournir au Canada un «plan de gestion des risques de la chaîne d'approvisionnement (SCRM)» qui décrit l'approche du fournisseur en matière de gestion des risques de la chaîne d'approvisionnement (SCRM) et montre comment l'approche du fournisseur en matière de SCRM réduira et atténuera les risques de la chaîne d'approvisionnement. Le plan SCRM doit être aligné sur l'une des meilleures pratiques suivantes et être évalué et validé par un tiers indépendant certifié en vertu de l'AICPA ou de CPA Canada et / ou du régime de certification ISO: (i) ISO / IEC 27036 Technologies de l'information - Techniques de sécurité - Sécurité de l'information pour les relations avec les fournisseurs (parties 1 à 4); (ii) Publication spéciale NIST 800-161 - Pratiques de gestion des risques liés à la chaîne d'approvisionnement pour les systèmes et organisations d'information fédéraux; ou (iii) le contrôle de sécurité ITSG-33 pour SA-12 lorsque l'organisation a défini des mesures de sécurité dans un plan SRCM.

(c) Nonobstant ce qui précède, le plan SCRM du fournisseur doit comprendre, au minimum:

(i) Un processus pour spécifier et concevoir l'infrastructure et les systèmes des fournisseurs suivant les processus d'ingénierie de sécurité afin qu'ils soient protégés contre les menaces externes et contre les vulnérabilités matérielles et logicielles;

(ii) Un processus pour déterminer les fonctions critiques et les techniques de protection (contre-mesures et sous-contre-mesures) utilisées pour assurer la protection du système pour tous les composants matériels et logiciels critiques utilisés tout au long de l'approvisionnement du fournisseur

(iii) les mécanismes de livraison physiques et logiques qui seront utilisés par le fournisseur et ses sous-traitants pour se protéger contre les incidents de sécurité;

(iv) les processus opérationnels (pendant la maintenance, la mise à niveau, les correctifs, le remplacement des éléments ou d'autres activités de maintien en puissance) et les processus d'élimination qui limitent les possibilités d'incidents de sécurité;

(v) La relation entre le fournisseur et tout fabricant d'un actif en tant que l'un des éléments suivants: (1) OEM; (2) revendeur agréé; (3) partenaire / distributeur autorisé; ou (4) source inconnue / non identifiée; et

(vi) Le programme de formation et de sensibilisation du SCRM du fournisseur.

(d) Le fournisseur doit fournir un plan SRCM à jour au Canada sur une base annuelle, ou immédiatement après tout changement important au plan SRCM.

(e) Le fournisseur doit fournir une liste des dispositifs de protection de périmètre (PPD) présents dans l'environnement des services. Les types de produits informatiques définis comme PPD sont des appareils informatiques qui peuvent appliquer (bloquer / refuser ou autoriser) le trafic IP en fonction de l'adresse IP, du port IP ou du type de protocole basé sur IP déployé à la frontière du réseau cloud du fournisseur de services cloud. Les dispositifs internes (derrière la limite) de protection du périmètre sont exclus de l'examen PPD de la chaîne d'approvisionnement. Sur demande, le fournisseur doit fournir au GC une liste des dispositifs de protection du périmètre (PPD) présents dans l'environnement des services dans les 10 jours ouvrables suivant la réception de toute demande, dans un format standard approuvé par le responsable technique.

34. Sous-traitants

(a) Le fournisseur doit fournir une liste de sous-traitants auxquels il pourrait faire appel pour exécuter n'importe quelle partie des travaux en fournissant le service au Canada. La liste doit comprendre les renseignements suivants : (i) le nom du sous-traitant; (ii) la description des travaux qui seraient exécutés par le sous-traitant; et (iii) les emplacements où le sous-traitant exécuterait les travaux.

(b) Le fournisseur doit fournir une liste des sous-traitants dans les dix jours suivant la date d'entrée en vigueur du contrat. Le fournisseur doit aviser le Canada (en mettant à jour le site Web et en fournissant au client un mécanisme lui permettant d'obtenir un avis lié à cette mise à

jour) au sujet de tout nouveau sous-traitant au moins 14 jours avant de fournir aux sous-traitants l'accès aux données du client ou aux données personnelles. Le fournisseur doit aider le Canada à mener les vérifications visant les sous-traitants dans les dix jours ouvrables.

Appendice E – Processus d'intégrité de la chaîne d'approvisionnement

1. Processus continu d'intégrité de la chaîne d'approvisionnement

(a) L'entrepreneur reconnaît que la sécurité est une considération critique pour le Canada en ce qui concerne ce contrat et qu'une évaluation continue des services nuages sera requise en ce qui concerne ce contrat.

(b) Les parties reconnaissent que le Canada se réserve le droit d'examiner les services nuage et les services de marché tiers de tout entrepreneur, en tout ou en partie, à tout moment pour des problèmes d'intégrité de la chaîne d'approvisionnement. Cette reconnaissance n'oblige pas l'entrepreneur à soutenir la révision du SCI.

(c) Pendant toute la durée du contrat et toute période facultative, l'entrepreneur doit fournir au Canada des renseignements concernant toute violation de données du réseau de l'entrepreneur dont il a connaissance, ce qui entraîne soit (a) tout accès illégal au contenu canadien stocké sur l'équipement de l'entrepreneur ou des installations, ou (b) tout accès non autorisé à ces équipements ou installations, dans les deux cas où cet accès entraîne la perte, la divulgation ou la modification du contenu du Canada en relation avec le changement de propriété, aux services nuage en vertu du présent contrat qui compromettraient l' intégrité, confidentialité, contrôles d'accès, disponibilité, cohérence ou mécanisme d'audit du système ou des données et applications du Canada.

2. Sous-traitants

(a) L'entrepreneur doit fournir une liste de sous-traitants qui pourraient être utilisés pour exécuter n'importe quelle partie des services en nuage en fournissant au Canada les services en nuage. La liste doit inclure les informations suivantes (i) le nom du sous-traitant; (ii) l'identification de la portée des activités qui seraient effectuées par le sous-traitant; et (iii) le pays (ou les pays) où le sous-traitant exécuterait les activités requises pour prendre en charge les services nuages

(b) L'entrepreneur doit fournir une liste de sous-traitants avant l'attribution du contrat, conformément aux formulaires ci-joints. L'entrepreneur doit fournir au Canada un avis (en mettant à jour le site Web et en fournissant au client un mécanisme pour obtenir un avis de cette mise à jour) de tout nouveau sous-traitant au moins 14 jours avant de fournir à ces sous-traitants un accès aux données du client ou aux données personnelles.

3. Changement de contrôle

(a) Si le Canada détermine, à sa seule discrétion, qu'un changement de contrôle affectant l'entrepreneur (soit à l'entrepreneur lui-même, soit à l'un de ses parents, jusqu'au propriétaire ultime) peut être préjudiciable à la sécurité nationale, le Canada peut résilier le contrat sur une «Sans faute» en fournissant un avis à l'entrepreneur dans les 90 jours civils suivant la réception de l'avis de

l'entrepreneur concernant le changement de contrôle. Le Canada ne sera pas tenu de fournir ses motifs de résiliation du contrat en relation avec le changement de contrôle, si le Canada détermine, à sa discrétion, que la divulgation de ces motifs pourrait elle-même porter atteinte à la sécurité nationale.

(b) Si le Canada détermine, à sa seule discrétion, qu'un changement de contrôle affectant l'entrepreneur (soit à l'entrepreneur lui-même, soit à l'un de ses parents, jusqu'au propriétaire ultime) peut être préjudiciable à la sécurité nationale, le Canada peut résilier le contrat sur une «Sans faute» en fournissant un avis à l'entrepreneur dans les 90 jours civils suivant la réception de l'avis de l'entrepreneur concernant le changement de contrôle. Le Canada ne sera pas tenu de fournir ses motifs de résiliation du contrat en relation avec le changement de contrôle, si le Canada détermine, à sa discrétion, que la divulgation de ces motifs pourrait elle-même porter atteinte à la sécurité nationale.

(c) (c) Dans le présent article, la résiliation sans faute signifie qu'aucune des parties ne sera responsable envers l'autre dans le cadre du changement de contrôle et de la résiliation qui en résulte, et le Canada ne sera responsable que du paiement des services reçus. jusqu'à la date effective de la résiliation.

(d) (d) Malgré ce qui précède, le droit du Canada de résilier sans faute ne s'appliquera pas aux circonstances dans lesquelles il y a une réorganisation interne qui n'affecte pas la propriété de la société mère ultime ou de la société mère de l'entrepreneur ou du sous-traitant , selon le cas; en d'autres termes, le Canada n'a pas le droit de résilier le contrat en vertu du présent article lorsque l'entrepreneur ou le sous-traitant continue, en tout temps, d'être contrôlé, directement ou indirectement, par le même propriétaire final.

FORMULAIRE 1

FORMULAIRE PRINCIPAL DE SOUMISSION DE L'IQ

Profil du répondant

Nom commercial légal du répondant («répondant»):	
Numéro et rue:	
Ville / Province:	
Code postal:	
Numéro de téléphone:	
Organisation mère (le cas échéant):	
Noms des membres du conseil d'administration ou des propriétaires:	
Numéro d'entreprise - approvisionnement (NEA):	
Personne-ressource principale de l'IQ	Nom: Titre: Courriel: Numéro de téléphone:
Le répondant est une entreprise autochtone au sens de l'annexe A (oui / non)	

Représentant du répondant

Nom et titre du ou des représentants du répondant	
Numéro et rue	
Numéros de téléphone (s)	
Courriel	
Langue préférée (Anglais ou Français)	

Membre de l’équipe du répondant

Nom et titre des membres de l'équipe	
Société (nom enregistré ou dénomination sociale)	
Adresse	
Numéros de téléphone (s)	
Courriel	
Langue préférée (Anglais ou Français)	

Membre de l’équipe du répondant

Nom et titre des membres de l'équipe	
Société (nom enregistré ou dénomination sociale)	
Adresse	
Numéros de téléphone (s)	
Courriel	
Langue préférée (Anglais ou Français)	

Membre de l’équipe du répondant

Nom et titre des membres de l'équipe	
Société (nom enregistré ou dénomination sociale)	
Adresse	
Numéros de téléphone (s)	
Courriel	
Langue préférée (Anglais ou Français)	

Membre de l’équipe du répondant

Nom et titre des membres de l'équipe	
Société (nom enregistré ou dénomination sociale)	
Adresse	
Numéros de téléphone (s)	
Courriel	
Langue préférée (Anglais ou Français)	

Membre de l’équipe du répondant

Nom et titre des membres de l'équipe	
Société (nom enregistré ou dénomination sociale)	
Adresse	
Numéros de téléphone (s)	
Courriel	
Langue préférée (Anglais ou Français)	

Copiez le tableau ci-dessus si vous proposez plus de cinq (5) membres de l'équipe.

Le représentant du répondant nommé ci-dessus déclare par les présentes en son nom propre et, pour plus de clarté, au nom de tous les membres de l'équipe du répondant:

a. il a le pouvoir et l'autorité de lier le répondant aux fins de l'IQ;

b. le Répondant est:
   - ☐ un propriétaire unique;
   - ☐ une responsabilité limitée ou une société en nom collectif;
   - ☐ une société; ou
   - ☐ un consortium non constitué en société exerçant des activités sous le nom du répondant susmentionné

c. s'il est invité à participer à la DDS, l'intimé préférerait recevoir la correspondance et les documents d'approvisionnement associés dans la langue suivante pendant le processus de DP. Veuillez sélectionner une (1) seule langue comme langue préférée du répondant:
   - ☐ Anglais
   - ☐ Français

d. ce formulaire de soumission de l'IQ principal n'a pas été modifié de quelque façon que ce soit, sauf pour inclure les informations requises du répondant et les informations de modification requises par ce formulaire; et

e. le répondant et ses sociétés affiliées respectent les dispositions relatives à l'intégrité énoncées à la section 5.1 - Dispositions relatives à l'intégrité, de l'IQ. En foi de quoi, le représentant du répondant a signé ce - Formulaire principal de soumission de l'IQ à la date indiquée ci-dessous.

Représentant du répondant:

Nom: _____

Titre: _____

Date: _____

_____
Signature

J'ai / Nous avons le pouvoir de lier le représentant du répondant et de lier le répondant et chaque membre de l'équipe du répondant.

FORMULAIRE 2

FORMULAIRE D'ATTESTATION DE L'ÉDITEUR DE LOGICIEL

(à utiliser lorsque le répondant est l'éditeur de logiciel)

Le répondant atteste qu'il est l'éditeur des logiciels et des composants de logiciel suivants et qu'il a tous les droits requis pour fournir les licences de ces logiciels (et de tous les sous-composants non exclusifs intégrés aux logiciels), libres de redevances pour le Canada:

_____

_____

_____

_____

_____

[*les* répondants *devraient ajouter ou retirer des lignes au besoin*]

Numéro de la demande de l'IQ: _____

Nom du répondant: _____

Signature du signataire autorisé du répondant: _____

Nom du signataire autorisé du répondant: _____

Titre du signataire autorisé du répondant: _____

Numéro de téléphone: _____

N° de l'invitation | Id de l'acheteur

HT300-193651/A | 052eem

Formulaire 3

Formulaire d'autorisation de l'éditeur de logiciel

(à utiliser lorsque le répondant n'est pas l'éditeur de logiciel)

Ceci confirme que l'éditeur de logiciels identifié ci-dessous a autorisé le répondant nommé ci-dessous à concéder sous licence ses produits logiciels propriétaires en vertu du contrat résultant de la demande de soumissions identifiée ci-dessous. L'éditeur de logiciels reconnaît qu'aucun emballage rétractable ou cliquable ou d'autres termes et conditions ne s'appliqueront, et que le contrat résultant de la demande de soumissions (tel que modifié de temps à autre par ses parties) représentera l'intégralité de l'accord, y compris en ce qui concerne à la licence des produits logiciels de l'éditeur de logiciels ci-dessous. L'éditeur de logiciels reconnaît en outre que si le mode de livraison (tel que le téléchargement) oblige un utilisateur à «cliquer» ou à reconnaître d'une autre manière l'application de conditions non incluses dans la demande de soumissions, ces conditions ne s'appliquent pas au Canada. l'utilisation des produits logiciels de l'éditeur de logiciels énumérés ci-dessous, même si l'utilisateur clique sur «J'accepte» ou signale de toute autre manière son accord avec les conditions générales supplémentaires.

Cette autorisation s'applique aux logiciels suivants:

_____

_____

[*les répondants devraient ajouter ou retirer des lignes au besoin*]

Nom de l'éditeur de logiciel (EL) _____

Signature du signataire autorisé de l'EL _____

Nom en caractères d'imprimerie du signataire autorisé de l'EL _____

Titre en caractères d'imprimerie du signataire autorisé de l'EL _____

Adresse du signataire autorisé de l'EL _____

N^{o} de téléphone du signataire autorisé de l'EL _____

N^{o} de télécopieur du signataire autorisé de l'EL _____

Date de signature _____

Numéro de la demande de soumissions _____

Nom du répondant _____