Canada Revenue Agency | Agence du revenu du Canada

DEMANDE DE RENSEIGNEMENTS (DR)

Nº 1000464174

SOLUTION DE GESTION DE LA FRAUDE D’ENTREPRISE

POUR

L’AGENCE DU REVENU DU CANADA

Date et heure de clôture: 29 Septembre 2023, à 14 h Heure Avancée de l'Est (HAE)

1.0 Avertissement

La réponse à la présente demande de renseignements ne constitue pas de condition préalable à la réception d'une demande de proposition (DDP) ou au droit d'y soumissionner pour cette exigence. Toute DDP sera affichée dans le Service électronique d'appels d'offres du gouvernement (SEAOG), communément appelé Achats Canada : (https://canadabuys.canada.ca)

Il ne faut pas interpréter la présente demande de renseignements comme une demande de soumissions ou de propositions. Aucun contrat ni autre forme d'engagement ne seront conclus en fonction des réponses à la présente demande de renseignements. Cette dernière n'est pas considérée comme une autorisation de l'Agence du revenu du Canada d'entreprendre des travaux qui entraîneraient des coûts pour l'Agence.

Rien dans la présente demande de renseignements ne sera considéré comme un engagement de l'Agence à présenter une DDP pour ce programme. L'Agence peut utiliser des renseignements non exclusifs donnés au cours de son examen ou dans la préparation de toute DDP officielle. L'ensemble des réponses seront conservées par l'Agence à titre confidentiel (sous réserve des lois fédérales applicables) et demeureront la propriété de l'Agence une fois reçues.

L'Agence peut reproduire, photocopier ou transcrire la réponse et toute documentation à l'appui non exclusive pour l'objet de cet examen ou l'inclusion dans tout document de DDP qui en découle. Nous conseillons aux fournisseurs qui répondent à la présente demande de renseignements d'indiquer clairement les parties de leur réponse qui sont exclusives et ils peuvent être invités à une réunion afin de clarifier davantage leurs réponses aux questions fournies à l'annexe A ci-jointe. La confidentialité des réponses de chaque fournisseur sera assurée.

L'Agence ne sera liée à aucun passage inclus dans le présent document. L'Agence se réserve le droit de modifier en tout temps une partie ou la totalité des exigences si elle le juge nécessaire. L'Agence se réserve aussi le droit de réviser son approche en matière d'approvisionnement, si elle le juge approprié, que ce soit à partir des renseignements soumis en réponse à la présente demande de renseignements ou pour toute autre raison qu'elle estime appropriée.

Les réponses à la présente demande de renseignements ne seront pas utilisées aux fins de qualification préalable et ne pourront en aucun cas restreindre la participation aux futurs processus d'approvisionnement (p. ex., dans le cas d'une demande de proposition). Les réponses ne seront pas évaluées de façon officielle.

L'Agence ne remboursera aucune dépense engagée pour la préparation des réponses et la participation aux séances de présentation liées à la présente demande de renseignements.

2.0 Séances de démonstration interactive

L'Agence peut, à sa seule discrétion, fournir des présentations et des démonstrations auprès des répondants intéressés afin de leur donner la possibilité de faire un suivi de leur réponse écrite pour faire état de leurs capacités en relation avec la présente demande de renseignements.

Les répondants qui ont manifesté un tel intérêt et qui ont démontré, au moyen de leur réponse à la demande de renseignements, que leurs produits correspondent suffisamment aux produits en question, comme il est indiqué dans le présent document, peuvent être contactés dans les deux semaines suivant la date de clôture de la demande de renseignements.

Les présentations et les démonstrations seront virtuelles en utilisant MS Teams.

Chaque séance sera d'un maximum de deux heures.

Les répondants doivent connaître les capacités des services pour répondre aux questions lors de la séance de présentation et de démonstration.

3.0 Réponses et demandes de renseignements

Les réponses aux questions doivent être soumises lorsqu'elles sont complètes et par écrit dans l'ordre indiqué. Toutes les demandes de renseignements dans toutes les sections du présent document doivent être traitées de façon concise, tout en fournissant tous les renseignements nécessaires pour comprendre la solution proposée. Tout écart par rapport à la demande ou aux exigences qui ne peuvent pas être respectées par le fournisseur doit être indiqué de façon claire.

Tous les renseignements confidentiels ou de nature exclusive contenus dans la réponse d'un fournisseur **doivent être clairement marqués « EXCLUSIF » ou « CONFIDENTIEL », par élément ou dans la partie supérieure de chaque page.**

Le fournisseur doit indiquer le nom, l'adresse électronique et le numéro de téléphone d'une personne-ressource dans sa réponse.

Les fournisseurs sont priés de soumettre leurs réponses à la présente demande de renseignements par courriel à l'adresse Shawn.Woods@cra-arc.gc.ca au plus tard le 29 septembre 2023 à 14h, Heure Avancée de l'Est (HAE). Les réponses reçues après cette échéance ne seront pas examinées. h

Les soumissions électroniques sont obligatoires et doivent être soumises sous la forme d'une trousse complète.

Toutes les questions en lien avec la présente demande de renseignements doivent être posées à Shawn Woods par courriel à l'adresse Shawn.Woods@cra-arc.gc.ca

4.0 Environnement opérationnel et technique actuel

L'Agence du revenu du Canada examine des solutions de rechange à son système actuel de gestion de la fraude d'entreprise (GFE).

Le système de GFE est défini comme un logiciel qui appuie la détection, l'analyse et la gestion de la fraude interne et de l'utilisation malveillante par les employés.

La solution actuelle de la GFE de l'Agence surveille et analyse les activités des utilisateurs dans les applications de l'Agence à l'aide du trafic sur le réseau saisi. Les alertes sont générées en temps réel lorsque les utilisateurs surveillés enfreignent les règles d'affaires élaborées par l'Agence pour détecter la fraude interne et l'utilisation malveillante.

La solution actuelle de la GFE de l'Agence permet également aux utilisateurs du système de GFE de rediffuser visuellement les sessions de l'utilisateur surveillé aux fins d'analyse. Pour plus de clarté, la rediffusion est une reproduction visuelle de ce que l'utilisateur surveillé a vu et a effectué dans l'application surveillée.

L'Agence cherche à en apprendre davantage sur les solutions actuelles disponibles et les pratiques exemplaires de l'industrie qui peuvent entrer, enregistrer et surveiller plus efficacement les transactions dans les applications de l'Agence.

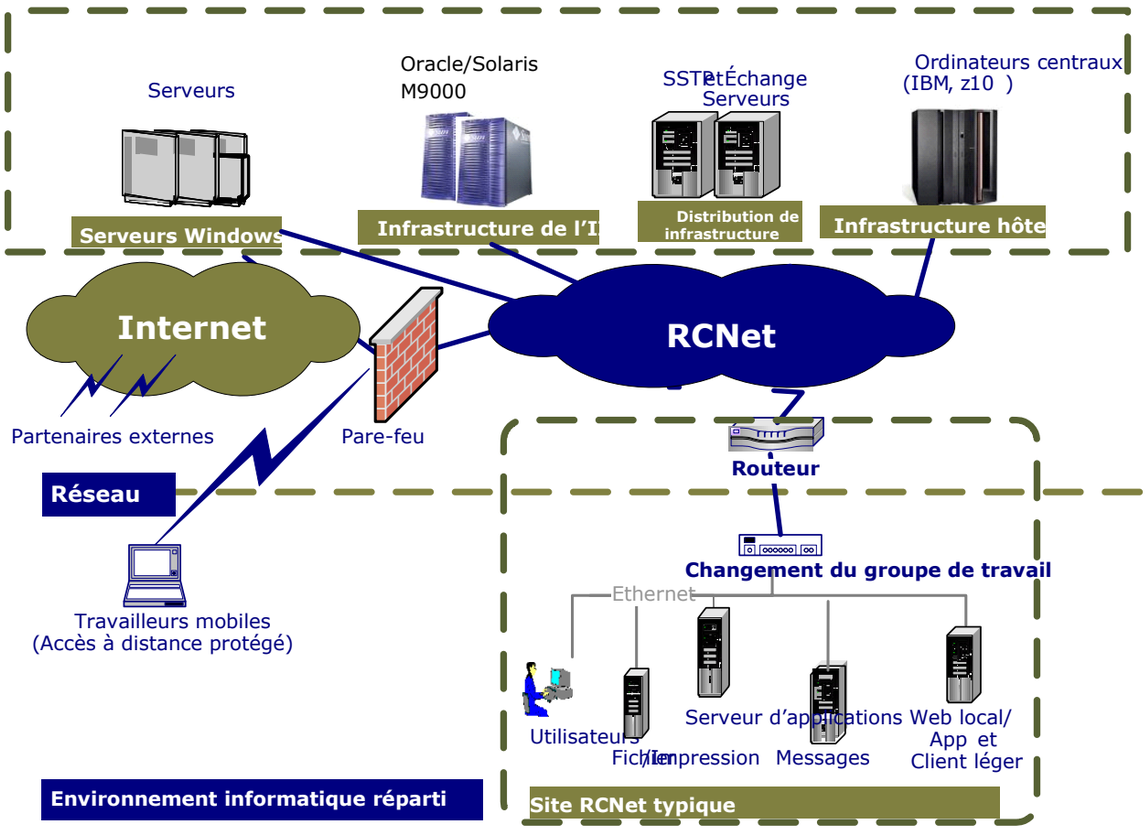
4.1 Aperçu général de l'infrastructure de Services partagés Canada et de l'Agence

L'infrastructure de Services partagés Canada (SPC) et de l'Agence compte deux centres de données qui hébergent cinq plateformes technologiques distinctes (c.-à-d. le matériel et les systèmes d'exploitation) :

A. Plateforme informatique répartie;
B. Plateforme Linux (c.-à-d. **infrastructure informatique d'affaires électroniques**);
C. zSeries;
D. Plateformes infonuagiques;
E. Plateforme d'intelligence d'affaires d'entreprise (serveur de rendement Netezza). Voir la figure 3.

Les deux centres de données fournissent actuellement des services d'infrastructure à l'Agence et à l'Agence des services frontaliers du Canada (ASFC). Consultez la **Figure 1** pour les représentations générales de l'infrastructure informatique de SPC et de l'Agence.

Figure 1 : Aperçu général de l'infrastructure informatique de SPC et de l'Agence



L'environnement informatique réparti

L'environnement informatique réparti (EIR) est une infrastructure client/serveur qui comprend des serveurs Windows, des ordinateurs de bureau, des ordinateurs portatifs et des tablettes avec Windows Active Directory fournissant les services de répertoire principaux.

Environ plus de 400 sites partout au Canada sont soutenus par l'EIR. La taille de ces sites variera, allant de quelques utilisateurs à des milliers dans un seul immeuble. La bande passante à ces sites varie également. Un site réparti type est formé d'un ou de plusieurs serveurs de fichiers et d'impression, de l'accès aux services de courriel Microsoft Exchange locaux ou centralisés, d'un contrôleur de domaine Active Directory et d'un certain nombre d'ordinateurs de bureau liés dans un réseau local.

L'Agence a également mis en œuvre la Plateforme technologique centralisée (PTC) à l'aide de Citrix XenApp 6.5, qui comprend des serveurs centraux situés dans la région de la capitale nationale et hébergeant diverses applications et divers services pour un groupe sélectionné d'utilisateurs finaux. Ces applications et ces services comprennent des applications de secteur d'activité précises ainsi que des applications de productivité de base, comme Microsoft Office, y compris Outlook, un émulateur d'hôte (Attachmate) et des services de fichiers et d'impression de base, pour n'en nommer que quelques-uns. De plus, l'Agence utilise la virtualisation des applications Softgrid pour améliorer l'accès et la gestion des applications au sein de la ferme de la PTC.

La PTC permet également d'accueillir les utilisateurs de l'accès à distance protégé (ADP) qui peuvent ne pas être sur un réseau étendu à l'échelle (RCNet) de l'Agence et de l'ASFC et qui se connectent à l'EIR au moyen de méthodes d'accès de rechange (p. ex., les fournisseurs de services Internet publics). La plateforme d'ADP est un sous-ensemble de l'EIR et est également fondée sur les systèmes d'exploitation Windows Server et Windows Client.

Les puces suivantes mettront en évidence les principaux logiciels Windows installés dans l'EIR de l'Agence et leurs mises à niveau prévues en fonction de la feuille de route actuelle de l'EIR de l'Agence.

- Microsoft Windows 2019 Server 64 bits;
- Citrix XenApp 6.5+;
- Microsoft Windows 10 (64 bits);
- Microsoft Exchange 2016;
- Microsoft Office 365;
- VMWare Sphere v4.x.

La version actuelle de l'environnement d'exécution Java installée sur chaque bureau est la version 1.8.x.

Le matériel sous-jacent pour l'environnement Windows est composé de serveurs basés sur des micro-dispositifs avancés et des architectures Intel utilisant une technologie à multi-cœurs et à multi-processeurs. Les ordinateurs de bureau et les

ordinateurs portatifs sont également fondés sur les architectures AMD et Intel qui utilisent des processeurs à un ou à multi-cœurs et une mémoire à deux canaux.

Infrastructure informatique d'affaires électroniques

La plateforme de l'infrastructure informatique d'affaires électroniques (IIAE) est une infrastructure informatique axée sur le service conçue pour héberger et soutenir les applications de l'Agence et de l'ASFC des essais unitaires à la production. Elle est formée d'une multitude de composantes et de services d'infrastructure, y compris le matériel de serveurs et de stockage, le serveur Web, le serveur d'intégration des applications, la messagerie, la connectivité des bases de données, la sécurité, les répertoires, la mise à l'essai des applications et la migration. Cette plateforme appuie un ensemble de normes technologiques fondées sur l'architecture de composantes Java.

Parmi les autres faits saillants de cette infrastructure informatique, on compte les suivants :

- Matériel de niveau 1 déployé aux fins de fiabilité;
- Utilisation, résilience et souplesse optimisées par l'utilisation des technologies de virtualisation;
- Conception axée sur la disponibilité élevée avec l'équilibrage de la charge et de la redondance entre deux centres de données, soutenus en tout temps (24 heures par jour, 7 jours par semaine);
- Soutien de l'architecture à trois étapes à l'aide de la technologie Enterprise Java Bean (EJB), et intégration aux composantes et aux services d'ordinateur central et répartis actuels;
- Surveillance et gestion de l'infrastructure en fonction des pratiques exemplaires de la bibliothèque de l'infrastructure de la technologie de l'information.

Les normes de base en matière de plateforme sont les suivantes :

- Matériel : serveurs x86;
- Virtualisation : VMWare ESX 5.0 ou RHEL KVM;
- Norme de système d'exploitation : RedHat Enterprise Linux 6.x, 7.9, 8.6;
- Serveur Web : Apache 2.2;
- Plateforme pour l'application Java : Oracle Weblogic 11g.

La plateforme zSeries

L'Agence exploite plusieurs machines IBM zSeries z196 Enterprise Class déployées dans deux (2) centres de données dans la région de la capitale nationale. Dans chaque centre de données, les machines sont regroupées dans des configurations parallèles Sysplex. Dans l'ensemble des centres de données, le Geographically Dispersed Parallel Sysplex (GDPS) d'IBM est actif pour la récupération des centres de données. La plateforme zSeries soutien l'exécution de l'un des systèmes d'exploitation z/OS, z/VM ou Linux.

L'environnement de configuration logique est composé des principaux composants de logiciels suivants :

- z/OS, version 1, lancement 13;
- DB2, versions 10, 11, 11.5;
- CICS/TS, version 4, lancement 1;
- Top Secret, version 15;
- ACF2, version 15.

Nuage

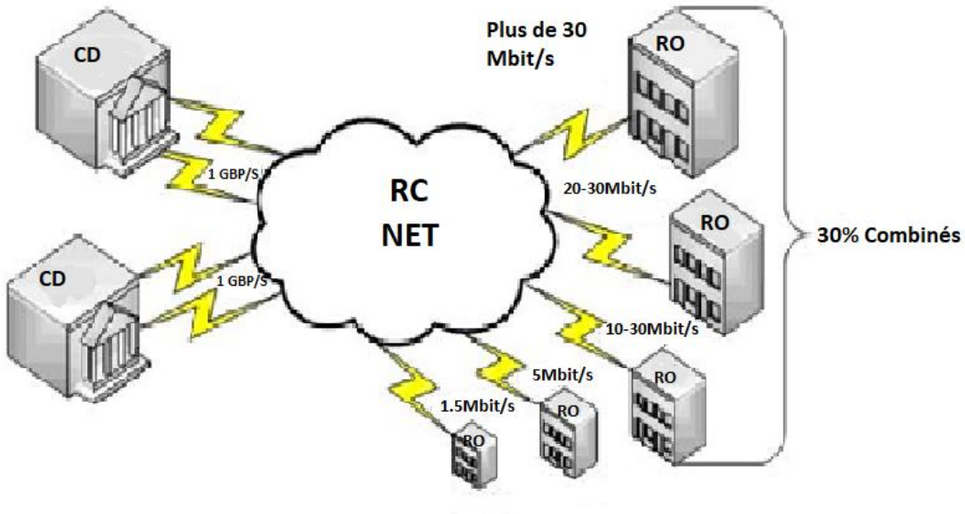
L'Agence a une présence en évolution dans le nuage en utilisant les principaux fournisseurs de services en nuage (p. ex., Amazon, Google, Microsoft). On s'attend à ce que l'Agence adopte un modèle d'infrastructure hybride avec un plus grand nombre d'applications en passant du sur place au nuage.

Environnement de réseau

Services partagés Canada exploite un RCN et pour l'Agence et l'ASFC qui s'étend à environ plus de 400 sites dans l'ensemble du Canada. RCNet installe des routeurs à protocoles multiples dans chaque immeuble pour interconnecter les segments du réseau local des utilisateurs et pour fournir un accès au réseau étendu. La majorité des immeubles sont interconnectés au moyen de circuits de la commutation multiprotocole par étiquette de 1,5 Mbit/s ou plus avec diverses configurations de qualité du service fondées sur le réseau. Le réseau privé virtuel de sécurité du protocole Internet (RPV IPSec) sur Internet en tant que circuit de secours est déployé dans la plupart de ces sites. À certains endroits éloignés, le RPV IPSec sur Internet (ligne d'abonné numérique, câble, satellite) est utilisé comme accès principal au réseau étendu.

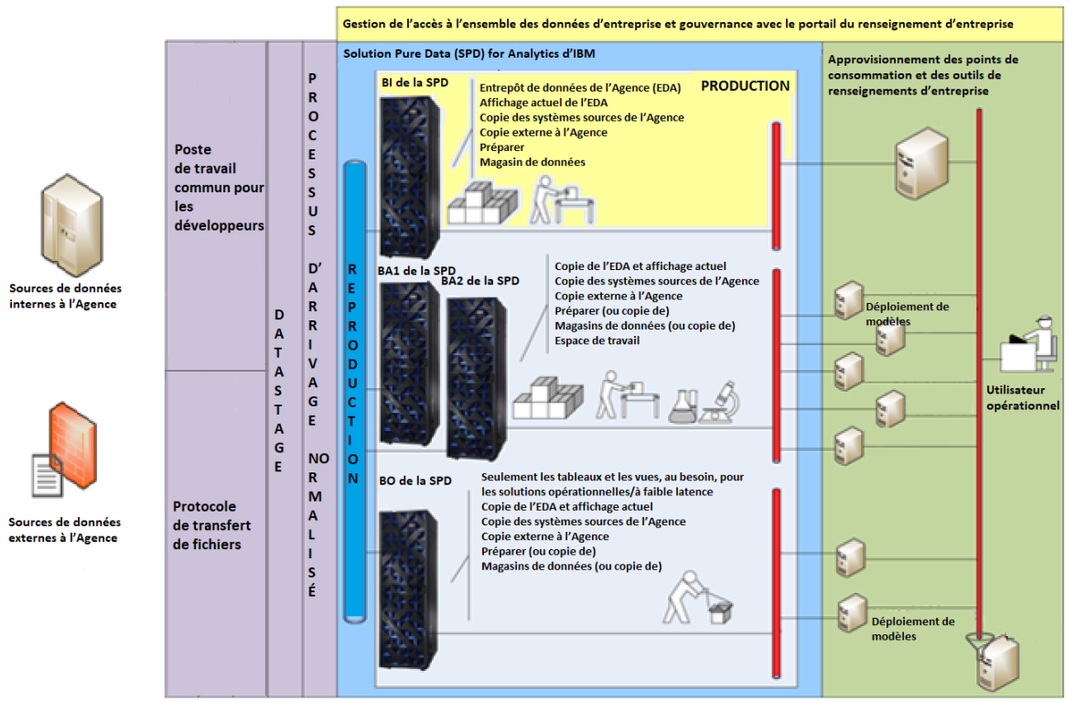
L'Agence exploite deux sites de production d'impression et de courrier à distance. La connectivité du réseau des centres de données utilise un pourcentage de la bande passante commune. L'utilisation moyenne des appels entrants à Summerside est de 2 Mbit/s. L'utilisation moyenne des appels entrants à Winnipeg est de 3,5 Mbit/s. Consultez la **Figure 2** pour les représentations générales de l'infrastructure de réseau.

Figure 2 : Infrastructure du réseau



CD = Centre de données
RO = Routeurs

Figure 3 : Plateforme d'intelligence d'affaires d'entreprise (serveur de rendement Netezza)



Le serveur de rendement Netezza remplace directement les appareils Pure Data for Analytics.

5.0 L'objectif de cette demande de renseignement consiste à :

1. Établir les capacités du fournisseur à fournir une solution de GFE qui peut répondre aux exigences de l'Agence.

2. Aider l'Agence à comprendre les normes, les pratiques exemplaires et les recommandations de l'industrie pour la détection, l'analyse et la gestion des risques de fraude et de l'utilisation malveillante des renseignements découlant de la consultation des employés et de la modification des renseignements confidentiels des contribuables.

3. Donner l'occasion à l'industrie de démontrer et de discuter de ses fonctionnalités, capacités et contraintes relatives aux logiciels.

4. Solliciter des rétroactions sur les possibilités d'intégration de la solution aux applications et aux systèmes de l'Agence.

5. Solliciter des rétroactions sur l'échéance, le niveau d'effort, les exigences en matière de matériel et l'architecture technique.

6.0 Contraintes dont il faut tenir compte pour la réponse

Langues officielles - Doit respecter la norme du gouvernement du Canada en vertu de la Loi sur les langues officielles, plus précisément les interfaces utilisateur, les fonctionnalités et la documentation en anglais et en français.

Accessibilité – Doit respecter la norme du gouvernement du Canada en vertu de la Loi canadienne sur l'accessibilité (accessible au moyen de l'hyperlien suivant Loi canadienne sur l'accessibilité (justice.gc.ca).

Pour ce faire, l'Agence a adopté la norme d'accessibilité EN 301 549 V3.2.1 (mars 2021) pour tous les produits et les services internes des technologies de l'information et des communications.

Renseignements personnels – Doit répondre à la norme du gouvernement du Canada, conformément à la Loi sur la protection des renseignements personnels (accessible en cliquant sur l'hyperlien suivant : http://laws-lois.justice.gc.ca/fra/lois/p-21/).

Résidence des données – Toutes les solutions SaaS hébergées dans le nuage doivent héberger les données au Canada.

Accès des utilisateurs – Doit prendre en charge la restriction de l'accès des utilisateurs (profils d'utilisateur) et de la configuration.

Intégration – Doit fournir un soutien pour la gestion des documents et des dossiers à l'interne ou à l'externe.

Conservation – Doit comprendre des règles flexibles de conservation des dossiers et des données.

7.0 Accessibilité

Promotion de l'accessibilité

La Loi canadienne sur l'accessibilité, qui a reçu la sanction royale en juin 2019, vise à favoriser la participation pleine et égale dans la société de toutes les personnes, en particulier les personnes en situation de handicap. Elle vise à parvenir à cette fin par la transformation progressive du Canada, dans le champ de compétence législative du Parlement, en un pays exempt d'obstacles, particulièrement par la reconnaissance, l'élimination et la prévention de ceux-ci.

L'Agence du revenu du Canada a un rôle à jouer dans la mise en œuvre de la vision d'un Canada accessible du gouvernement du Canada, et elle participe à l'acquisition de biens et de services qui facilitent l'exécution de programmes et la prestation de services visés par la Loi canadienne sur l'accessibilité.

L'Agence s'est engagée à faire preuve de leadership en ce qui concerne l'acquisition de biens et de services accessibles et à contribuer à l'objectif d'inclusion dès la conception et d'accessibilité par défaut. Comme il est prévu que cette initiative se déroule progressivement, les fournisseurs devraient s'attendre à ce que les exigences d'accessibilité dans les contrats d'approvisionnement du Canada évoluent et deviennent plus exigeantes au fil du temps.

Pour ce faire, l'Agence a adopté la norme d'accessibilité EN 301 549 V3.2.1 (mars 2021) pour tous les produits et les services internes des technologies de l'information et des communications.

8.0 Annexe A – Questions

Les questions suivantes représentent le type de renseignement que cherche l'Agence alors qu'elle étudie la façon dont il faut structurer toute demande de propositions suivant ce processus de demande de renseignements.

Cette liste de questions n'est pas exhaustive Les répondants sont invités à fournir tout renseignement supplémentaire qui pourrait être utile et avantageux pour l'ARC dans la préparation de toute DDP ultérieure.

QUESTIONS SUR L'ACCESSIBILITÉ	
A.1.1	La solution est-elle EN 301 549 V3.2.1 (2021-03) Norme européenne harmonisée respectée?
A.1.2	Y a-t-il un rapport de conformité en matière d'accessibilité fondé sur un modèle d'accessibilité volontaire aux produits (VPAT®) [de préférence VPAT® 2.4, Rev EU ou Rev INT] pour la solution?
A.1.3	Si la solution ne répond pas entièrement aux exigences de la norme EN 301 549, la feuille de route du produit comprend-elle des améliorations en matière d'accessibilité? Si oui, quel niveau de conformité sera atteint et à quelle date cible?

QUESTION SUR LE DÉVELOPPEMENT DURABLE	
Article 1.1	Votre organisation a-t-elle mis en place une politique environnementale d'entreprise? Dans l'affirmative, veuillez décrire les politiques et les procédures en place qui intègrent le développement durable dans ses activités pour : i) réduire les répercussions environnementales; ii) faire preuve de responsabilité sociale; et iii) contribue au bien-être économique et social des Canadiens.

QUESTIONS D'AFFAIRES	
B.1.1	Votre solution utilise-t-elle une « technologie d'écoute » de réseau passif ou une technologie semblable? Si oui, veuillez les décrire.
B.1.2	Votre solution empêche-t-elle les utilisateurs surveillés d'accéder à certains renseignements de façon proactive ou peut-elle afficher un message d'avertissement si l'accès porte atteinte à règles opérationnelles (considéré comme une utilisation malveillante ou frauduleuse)?
B.1.3	Expliquez à quel point votre solution permet d'entrer l'activité des utilisateurs aux fins d'analyse (p. ex., en temps quasi réel, pendant la nuit).
B.1.4	Décrivez et déterminez toutes les capacités d'alerte de votre solution lorsque l'activité ou le comportement de l'utilisateur est suspect (y compris les filtres, les déclencheurs, la notation des risques, etc.).
B.1.5	Décrivez comment votre solution peut rechercher rapidement de grands volumes de données saisies.
B.1.6	Décrivez comment règles opérationnelles peut être appliqué aux activités des utilisateurs saisis.
B.1.7	Décrivez comment votre solution surveille et analyse les utilisateurs privilégiés (utilisateurs auxquels sont accordés des pouvoirs administratifs) ainsi que les comptes génériques (un compte utilisé par plusieurs utilisateurs).
B.1.8	Décrivez comment votre solution fournit des capacités de gestion de la charge de travail et des cas ou la capacité d'intégrer d'autres produits de gestion de la charge de travail et des cas de tiers. Quelles sont les interfaces utilisateur disponibles (p. ex., interface utilisateur graphique [GUI], portails Web)?
B.1.9	Décrivez comment votre solution permet aux utilisateurs du système de la gestion de la fraude d'entreprise (GFE) d'associer, de stocker et de tenir à jour les rapports sur le flux de travail et d'autres documents. Quels types de documents et de dossiers votre solution prend-elle en charge et traite-t-elle?
B.1.10	Décrivez vos capacités d'établissement de rapports sur les solutions. • Déterminez tous les rapports prêts à l'emploi fourni (p. ex., incitatifs, en cascade, statistiques, etc.). • Déterminez tous les formats de fichiers de sortie générés par la fonction d'établissement de rapports de la solution (p. ex., PDF, Excel, HTML, XML, format CSV, etc.). • Votre solution fournit-elle un moteur de rapports personnalisable ou un kit de développement de logiciels (SDK)?
B.1.11	Fournissez deux exemples où votre solution a été mise en œuvre. Ces exemples doivent être de taille et de portée semblables à celles de l'Agence, comme il est décrit à la section 4.1 de la demande de renseignements. Précisez la durée de la mise en œuvre, les principaux facteurs de succès et les obstacles liés à la normalisation de cette solution.
B.1.12	Décrivez les mesures de protection que votre solution a mises en place pour protéger l'intégrité des données saisies (nécessaire pour assurer la non-répudiation lorsque mesure judiciaire est requis).

B.1.13	Décrivez les types de règles opérationnelles ou d'autres analyses que votre solution utilise pour repérer la fraude ou l'utilisation malveillante des renseignements.
B.1.14	Décrivez votre modèle de licence et d'établissement des coûts pour une plateforme infonuagique et une solution sur place.
B.1.15	Décrivez toute autre fonction ou offre clé de votre solution proposée dont l'Agence pourrait tirer parti et qui n'a pas été indiquée dans la présente demande de renseignements, ainsi que tout commentaire ou suggestion concernant l'approche de l'Agence pour atteindre son objectif.

QUESTIONS TECHNIQUES	
T.1.1	Déterminez toutes les plateformes, le matériel et les composants logiciels pris en charge par votre solution pour entrer les activités des utilisateurs. Par exemple, la façon dont votre solution surveille l'utilisation des éléments suivants : • Applications COBOL et CICS dans l'environnement z/OS; • Application MS Windows dans les environnements MS Windows/Citrix; et • Applications Linux/Unix dans un environnement Linux/Unix.
T.1.2	1. Décrivez les données que votre solution saisit auprès de l'utilisateur sur plusieurs canaux de communication au sein d'une infrastructure filaire et sans fil (p. ex., Web, mobile, médias sociaux, appels téléphoniques, etc.), les applications et les plateformes comprennent tout support ou périphérique portatif connecté localement dans cette description (p. ex., clés USB, imprimantes, etc.). Par exemple, lorsqu'un utilisateur consulte ou modifie des renseignements, la solution entrera-t-elle l'utilisateur, la requête, le champ qui a été modifié et le contenu avant et après de ce champ? 2. Votre solution enregistre-t-elle les écrans consultés par l'utilisateur dans les applications et les plateformes décrites à la section 4.1 de la demande de renseignements et rejoue-t-elle visuellement la session de l'utilisateur aux fins d'examen et d'analyse? Décrivez comment votre solution ferait cela.
T.1.3	Décrivez toutes les modifications de code ou de configuration que les applications développées par l'Agence devraient apporter pour fonctionner avec votre solution, y compris la façon dont elles seraient intégrées à votre solution dans le but d'entrer l'activité des utilisateurs afin d'appliquer le code règles opérationnelles pour détecter la fraude interne et l'utilisation malveillante des renseignements. Remarque : Cette description doit comprendre les modifications apportées aux applications ou aux plateformes existantes (p. ex., correctifs et ensembles de services).
T.1.4	1. Quelle quantité de données (en Go) votre solution peut-elle entrer et stocker quotidiennement si elle était utilisée pour surveiller et enquêter sur le comportement d'environ 40 000 utilisateurs surveillés? Peut-elle traiter des milliards de transactions par jour ou a-t-elle des limites ou des difficultés à traiter de grands volumes de données? 2. Décrivez comment votre solution s'adapte à l'augmentation des capacités, des utilisateurs et du rendement. Veuillez préciser les « plafonds » de croissance dans votre solution.
T.1.5	Décrivez comment les composantes d'alerte, de production de rapports et de gestion de la charge de travail de votre solution sont intégrées.
T.1.6	Décrivez comment votre solution s'intègre aux applications Java (client Swing, clients Web et EJB).
T.1.7	1. Quelles versions de TLS/SSL votre solution peut-elle déchiffrer à partir du trafic hôte surveillé saisi? 2. Quelle infrastructure est nécessaire pour déchiffrer les versions de chiffrement prises en charge?
T.1.8	Quels protocoles exclusifs sont pris en charge (p. ex., T3, file d'attente de MQ)?
T.1.9	Décrivez la façon dont votre solution envoie et reçoit des données à partir d'autres applications commerciales prêtes à l'emploi ou de solutions partenaires.
T.1.10	Votre solution interprète-t-elle plusieurs saisies/transactions afin de déterminer les actions de l'utilisateur au cours d'une période donnée? Si c'est le cas, décrivez comment cela est accompli. Comment les sources de données multiples sont-elles intégrées à la reconstitution de l'événement?
T.1.11	Décrivez comment votre solution permet d'établir des relations à l'aide de données transactionnelles saisies avec d'autres sources de données (internes et externes à votre solution) afin d'appliquer le code règles opérationnelles.
T.1.12	Décrivez comment votre solution importe les données de sources externes (p. ex., les données historiques sur les activités des utilisateurs, comme les enregistrements de pistes de vérification) aux fins d'utilisation avec votre moteur règles opérationnelles.
T.1.13	Décrivez comment votre solution saisit et utilise les transactions des utilisateurs de bout en bout chiffrées pour le traitement règle opérationnelle.

T.1.14	Si votre solution contient des dépendances de source ouverte, ces bibliothèques sont-elles tenues à jour? Et comment?
T.1.15	1. Combien de temps après le lancement d'une version importante d'un système de gestion de base de données (PG, MSSQL, DB2) votre produit prend-il en charge cette nouvelle version? 2. Votre application permet-elle la mise à jour des versions mineures du système de gestion des bases de données sans mise à niveau?
T.1.16	Quelle est la durée de votre période de soutien pour les versions majeures? Veuillez nous faire part de toutes les feuilles de route disponibles qui les décrivent.
T.1.17	Quelles méthodes votre solution utilise-t-elle pour sécuriser et protéger l'accès à ses composantes et à ses données (p. ex., authentification, autorisation, journaux de vérification, Active Directory, etc.), et les droits peuvent-ils être limités à des rôles fonctionnels définis?
T.1.18	Quelle est votre méthode d'application des correctifs et votre calendrier pour les correctifs de sécurité?
T.1.19	Quelles répercussions sur les ressources de l'infrastructure une organisation devrait-elle connaître lors du déploiement de sa solution (p. ex., traitement, bande passante, stockage, etc.)?
T.1.20	Décrivez comment votre solution prévoit le développement, la mise à l'essai et la mise au point de règles opérationnelles avant leur migration vers la production.
T.1.21	1. Décrivez vos offres de maintenance et de soutien (p. ex., avant le déploiement, après le déploiement, la consultation de soutien après les heures normales de travail, le soutien sur appel 7 jours sur 7, 24 heures sur 24, etc.), la façon dont elles sont fournies et les échéanciers prévus. 2. Votre organisation a-t-elle établi des niveaux de service?
T.1.22	1. Décrivez les activités, ainsi que la nature et le niveau d'expertise requis afin de maintenir la solution de façon continue. 2. Décrivez les trousses de formation fournies (p. ex., manuels en ligne, soutien, aide, méthodes et procédures). 3. Offrez-vous des cours de formations standards et personnalisées?
T.1.23	1. Lorsqu'une organisation remplace une solution de GFE existante par votre solution, veuillez décrire le calendrier de mise en œuvre et la façon dont votre solution permettrait la migration ou la réutilisation des règles de détection de la fraude existantes, des travaux et des tâches automatisés, des données saisies et du matériel à votre solution tout en réduisant au minimum les interruptions de travail. 2. Quelle serait votre approche recommandée pour réduire au minimum les interruptions de travail? Votre entreprise peut-elle fournir de l'aide ou des ressources à la mise en œuvre (aide à la mobilisation) afin de gérer la transition?

QUESTIONS TECHNIQUES – LIÉES AU NUAGE	
T.2.1	Quel type de capacités de surveillance et d'enregistrement votre application offre-t-elle dans un environnement infonuagique?
T.2.2	1. Lorsque les hôtes surveillés résident à la fois sur place et dans le nuage (modèle hybride), comment votre logiciel centralise-t-il les données et permet-il d'analyser ces données? 2. Quelle méthode sécurisée votre solution a-t-elle pour échanger des données entre les hôtes sur place et dans le nuage?
T.2.3	Quelle est votre stratégie pour traiter : 1. Les exigences en matière de confidentialité, de sécurité et de conformité des données pour votre application et les données stockées dans un environnement infonuagique? 2. Décrivez comment votre solution répond à la norme du gouvernement du Canada en vertu de la Loi sur la protection des renseignements personnels.
T.2.4	Comment gérez-vous la gestion de la configuration et l'automatisation de l'infrastructure pour votre application dans un environnement infonuagique?
T.2.5	Quelles sont les options de reprise après sinistre et de sauvegarde pour votre application dans un environnement infonuagique?
T.2.6	Est-ce que votre logiciel a des dépendances ou des exigences qui pourraient avoir une incidence sur son rendement dans un environnement infonuagique?
T.2.7	Votre solution permet-elle d'héberger les données exclusivement au Canada?