Pièce jointe A – Énoncé de défi (partiel)

(Remarque à l'intention des soumissionnaires : Une version finale de l'Énoncé de défi, des pièces jointes et annexes sera ajoutée lors de la Sollicitation par défis d'une offre à commandes finale).

Contexte

Comme cela est indiqué dans le *Plan stratégique des opérations numériques du gouvernement du Canada*, le gouvernement du Canada (GC) travaille à fournir des réseaux et une infrastructure fiables tout en renforçant la sécurité du réseau en passant à un réseau d'entreprise unique, moderne et de bout en bout auquel les utilisateurs peuvent accéder en tout temps et de n'importe où. L'intégrité et la sécurité des données et de l'infrastructure de la technologie de l'information (TI) du gouvernement du Canada sont essentielles à la prestation de services offerts à la population canadienne. Comme les cyberattaques sont de plus en plus sophistiquées et fréquentes, le GC doit rester vigilant et continuer à renforcer ses défenses. Le gouvernement a mis en place des services de surveillance et des mesures défensives de classe mondiale à son périmètre de réseau au moyen de passerelles gérées par Services partagés Canada (SPC). Cependant, toutes les organisations du GC ne bénéficient pas de ces services.

Énoncé du problème

Le Canada ne dispose pas d'une solution de sécurité infonuagique d'entreprise qui lui permette d'offrir une expérience utilisateur uniforme à partir de n'importe quel appareil, en tout lieu et à tout moment.

Dans certains cas, le Canada n'est doté d'aucun contrôle de sécurité uniforme et rentable pour protéger ses données et ses actifs sur les sites éloignés des ministères, ainsi que les utilisateurs éloignés (du GC et autres), y compris les petits ministères et organismes (PMO), lorsqu'ils accèdent à Internet, à des logiciels en tant que service (SaaS) en nuage, à des infrastructures en tant que service (IaaS), à des plateformes en tant que service (PaaS) et aux services sur place du GC. De cette situation découlent une perte de productivité, une hausse des coûts, une baisse de la satisfaction et du moral des utilisateurs, une augmentation des risques en matière de cybersécurité et un manque d'uniformité de l'expérience de l'utilisateur.

Le Canada souhaite améliorer et optimiser la capacité d'utiliser et de fournir en toute sécurité des services basés sur le nuage de manière efficace, efficiente et rapide en utilisant une solution de sécurité basée sur le nuage et fondée sur les SaaS. Celle-ci aidera le Canada à cheminer vers une approche à vérification systématique qui permet de répondre au besoin du Canada de maintenir la visibilité et la sécurité de son accès à Internet et au nuage tout en améliorant la performance du réseau et l'expérience de l'utilisateur.

Défis spécifique à la solution

Les problèmes que doit résoudre la solution de services de sécurité infonuagique (SSI) peuvent se résumer comme suit :

- Un manque d'uniformité de la performance et de l'expérience utilisateur en ce qui concerne l'accès aux IaaS, aux SaaS et aux PaaS fondés sur le nuage public.

- L'utilisation d'une connexion directe à Internet pour accéder au nuage public ou aux services sur place du GC expose le GC et les ministères à des menaces. Ceci concerne les utilisateurs situés sur des sites éloignés et dans des bureaux à domicile, ainsi que les utilisateurs mobiles. Ces « périmètres » doivent être protégés de manière appropriée.

- Les coûts élevés associés au réacheminement du trafic Internet vers les centres régionaux du GC par l'intermédiaire de circuits MPLS (commutation de labels multiprotocole). Les coûts comprennent généralement le circuit MPLS, le coût des circuits Internet dans les centres régionaux de Service Internet d'entreprise (SIE) de SPC pour ce trafic, ainsi que l'augmentation de la pile de sécurité dans les centres régionaux existants. En ce qui concerne l'accès direct à Internet, il est également coûteux de fournir une pile de sécurité approuvée par le GC à chaque site éloigné qui dispose d'un accès direct à Internet.

- Un manque d'uniformité des services de sécurité du périmètre sur les sites éloignés, ainsi qu'au sein de certains ministères partenaires de SPC et des PMO.

Définitions

- **Doit pouvoir** – Fonction ou composante de la solution qui doit être offerte aux utilisateurs.

- **Utilisateur mobile** – Un utilisateur du GC en déplacement avec un ordinateur portable, qui peut travailler de n'importe quel endroit, y compris, mais sans s'y limiter, de son domicile, d'un hôtel, d'un café, etc.

- **Site éloigné du GC** – Un bâtiment ou des locaux à bureaux du GC occupés par des employés, des experts-conseils ou des entrepreneurs du GC.

- **Logiciel d'utilisateur final de la solution de SSI** – Comprend tout logiciel lié aux SSI, tel qu'un agent/client de la solution de SSI, des extensions de navigateur, etc., qui est installé sur un ordinateur portable ou de bureau d'un utilisateur final.

- **Agent de la solution de SSI** – Application logicielle de point d'extrémité de la solution de SSI (agent ou client) qui est installée sur l'appareil d'un utilisateur final.

- **Appareil géré** – Un ordinateur portable ou de bureau qui appartient au GC et est géré par celui-ci. Le logiciel d'utilisateur final de la solution de SSI peut être installé sur ce genre d'appareil à la

discrétion du GC ou d'un de ses ministères. Un certificat d'appareil du GC est généralement installé sur les appareils gérés.

- **Appareil non géré par le GC** – Un ordinateur portable ou de bureau d'une organisation externe (qui n'est pas du GC) qui n'appartient pas au GC et n'est pas géré par celui-ci. L'installation de tout logiciel d'utilisateur final de la solution de SSI sur des appareils non gérés par le GC est à la discrétion de l'organisation de l'extérieur du GC qui possède ou gère l'ordinateur portable ou de bureau. Le GC peut avoir une influence sur l'installation du logiciel d'utilisateur final de la solution de SSI sur ces appareils. Un exemple d'appareil non géré par le GC est un ordinateur portable détenu et géré par un service de recherche universitaire qui fait affaire avec le GC.

- **Apportez votre propre appareil** – Un ordinateur portable ou de bureau personnel détenu et géré par un utilisateur final. Le logiciel d'utilisateur final de la solution de SSI peut être installé sur ces appareils à la discrétion de l'utilisateur final. Le GC n'aura probablement aucune influence sur l'installation du logiciel de la solution de SSI sur ces appareils qui devraient être considérés comme sans agent ou sans client.

- **Internet des objets (IO) et appareil scientifique** – Un appareil informatique dans lequel sont intégrés des capteurs, une capacité de traitement, des logiciels et d'autres technologies qui se connectent et échangent des données avec d'autres appareils et systèmes. Un appareil scientifique est souvent contrôlé par un utilisateur avec un plus grand niveau d'interaction avec un utilisateur qu'un appareil de l'IO. La capacité d'installer un logiciel d'utilisateur final de la solution de SSI sur les appareils de l'IO et scientifiques peut être limitée ou inexistante.

- **Utilisateur externe** – Un utilisateur qui n'est pas un employé du GC à quelque titre que ce soit, mais qui a besoin d'accéder aux applications, aux données ou aux services du GC. Un chercheur universitaire, employé par l'université, qui collabore avec un organisme de recherche du GC est un exemple d'utilisateur externe.

- **Multilocation** – Une seule instance du logiciel et de son infrastructure de soutien peut servir plusieurs clients. Chaque client partage l'application logicielle et également une base de données unique. Les données de chaque locataire sont isolées et restent invisibles pour les autres locataires.

- **Logiciel en tant que service (SaaS)** – Une solution SaaS est définie comme étant un logiciel appartenant à un ou plusieurs fournisseurs, qui le livrent et le gèrent à distance. Le fournisseur fournit des services de logiciel d'après un ensemble commun de définitions de code et de données qui est utilisé en tout temps par tous les clients sous contrat, dans un modèle un à plusieurs, selon le principe du paiement à l'utilisation ou sous forme d'abonnement en fonction des paramètres d'utilisation.

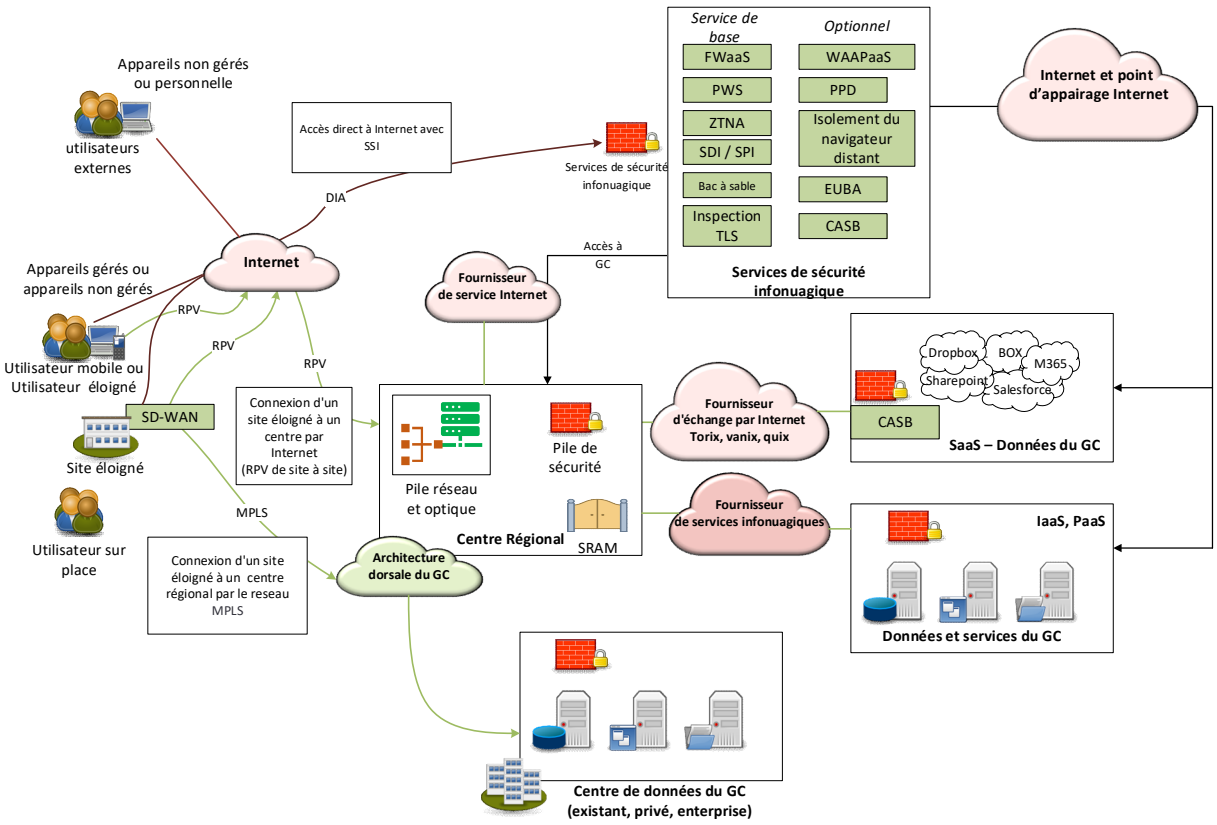
- **Fournisseur** – L'entrepreneur qui fournit la solution dans le cadre du présent contrat.

- **Organisation parent** – Une organisation de niveau supérieur qui a des niveaux de contrôle, de visibilité et d'accès à tous les renseignements de l'organisation subordonnée et des unités opérationnelles subordonnées ainsi qu'aux siens.

- **Organisation enfant** – Une organisation subordonnée qui a des niveaux de contrôle, de visibilité et d'accès uniquement aux renseignements de sa propre unité opérationnelle de l'organisation et des unités opérationnelles subordonnées et pas à d'autres.

Architecture générale proposée

Le diagramme qui suit illustre l'architecture générale de la solution de SSI :



Cas d'utilisation fondés sur l'architecture générale proposée

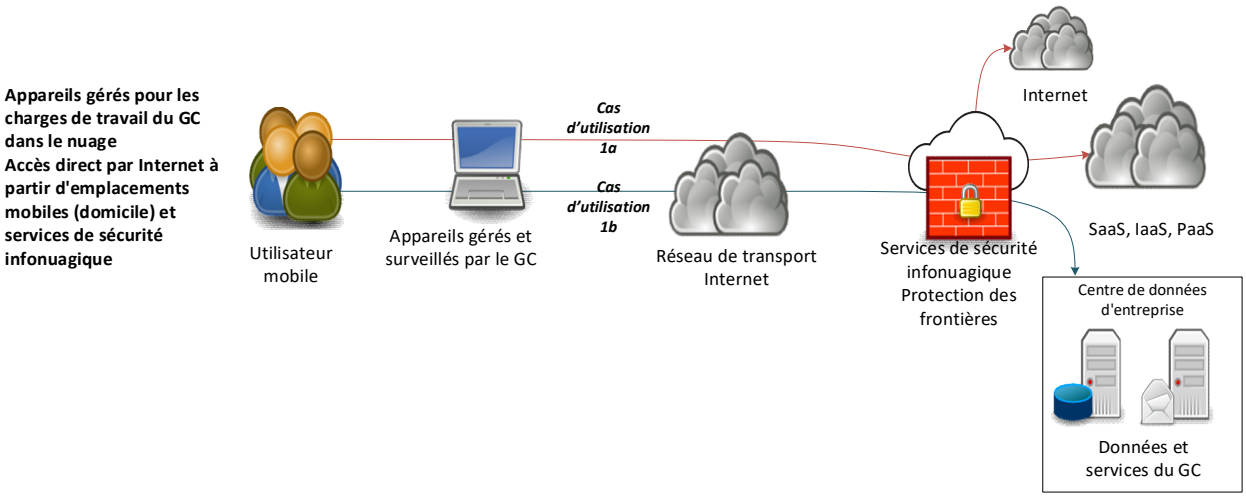
Les cas d'utilisation suivants constituent l'environnement opérationnel dans lequel SPC a l'intention de tirer parti de la solution de SSI.

1. Cas d'utilisation 1a : utilisateur mobile (appareil géré) accédant aux services infonuagiques

Un utilisateur mobile du GC équipé d'un appareil géré accède aux services infonuagiques de l'extérieur des bureaux du GC (à la maison, à l'hôtel, par l'entremise d'une connexion Internet publique, etc.) Tout le trafic de l'utilisateur passe par un tunnel chiffré sécurisé depuis le point d'extrémité de l'utilisateur vers la solution de SSI, puis vers la destination dans le nuage public (accès général à Internet, SaaS, IaaS ou PaaS).

Cas d'utilisation 1b : utilisateur mobile (appareil géré) accédant aux services sur place du GC (centre de données d'entreprise ou CDE)

Un utilisateur mobile du GC équipé d'un appareil géré accède aux services sur place du GC de l'extérieur des bureaux du GC (à la maison, à l'hôtel, par l'entremise d'une connexion Internet publique, etc.), de façon protégée grâce aux services de sécurité de la solution de SSI. Tout le trafic de l'utilisateur passe par un tunnel chiffré sécurisé depuis le point d'extrémité de l'utilisateur vers la solution de SSI, puis vers la destination dans un CDE du GC.

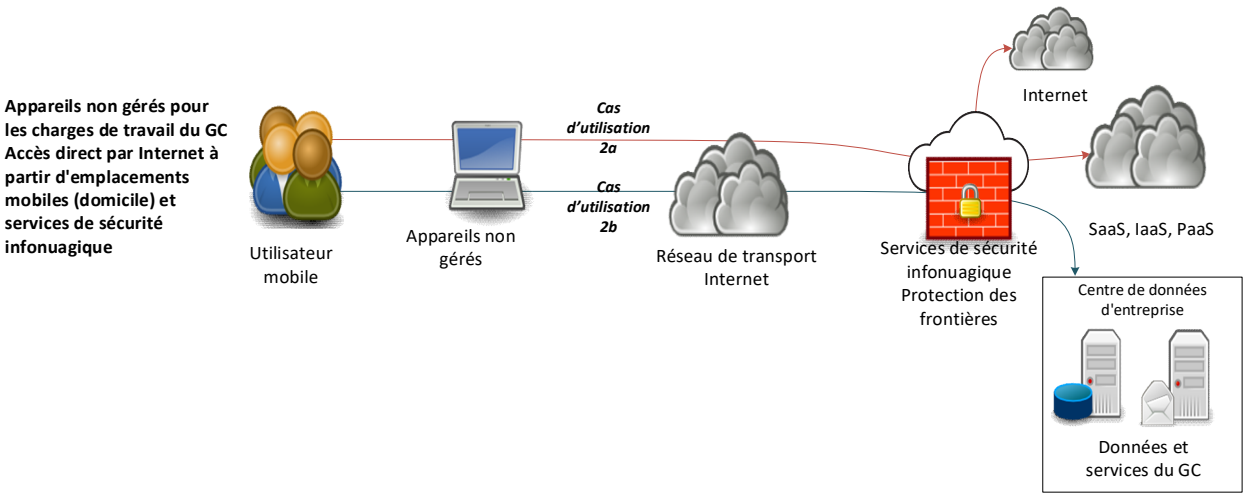


2. Cas d'utilisation 2a : utilisateur mobile (appareil non géré par le GC) accédant aux services infonuagiques

Un utilisateur mobile du GC équipé d'un appareil non géré par le GC accède aux services infonuagiques de l'extérieur des bureaux du GC (à la maison, à l'hôtel, par l'entremise d'une connexion Internet publique, etc.) Le trafic vers des applications et des services particuliers du GC passe par un tunnel chiffré sécurisé depuis le point d'extrémité de l'utilisateur vers la solution de SSI, puis à la destination dans le nuage public (p. ex., SaaS, IaaS ou PaaS). L'accès à des applications ou à des services qui ne sont pas spécifiquement identifiés (p. ex., la navigation générale sur Internet) ira directement sur Internet, en contournant la solution de SSI.

Cas d'utilisation 2b : Utilisateur mobile (appareil non géré par le GC) accédant aux services sur place du GC (CDE)

Un utilisateur mobile du GC muni d'un appareil non géré par le GC accède aux applications et services sur place du GC de l'extérieur des bureaux du GC (à la maison, à l'hôtel, par l'entremise d'une connexion Internet publique, etc.) Le trafic vers des applications et des services particuliers du GC passe par un tunnel chiffré sécurisé depuis le point d'extrémité de l'utilisateur vers la solution de SSI, puis à la destination dans un CDE du GC.

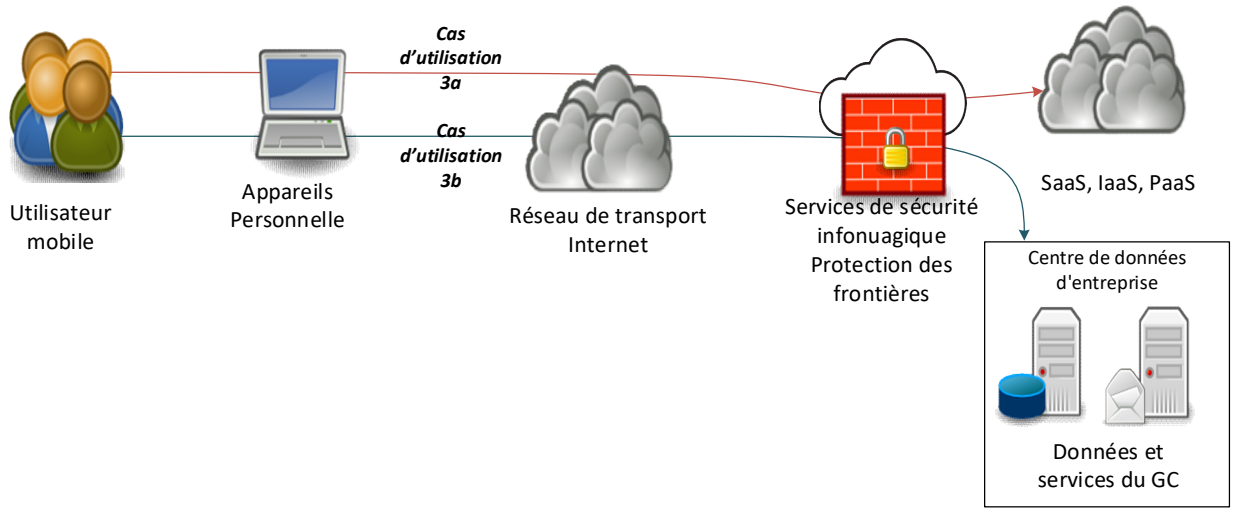


3. Cas d'utilisation 3a : Utilisateur qui accède à des services infonuagiques à l'aide de son propre appareil

Un utilisateur mobile du GC qui utilise son propre appareil, sans avoir la possibilité d'installer un logiciel de SSI, accède à des services infonuagiques à l'extérieur des bureaux du GC (à la maison, à l'hôtel, par l'entremise d'une connexion Internet publique, etc.) protégé par des services de sécurité au sein de la solution de SSI. Le trafic vers des applications et des services particuliers du GC passe par un tunnel chiffré sécurisé depuis le point d'extrémité de l'utilisateur vers la solution de SSI, puis à la destination dans le nuage public (p. ex., SaaS, IaaS ou PaaS). L'accès à des applications ou à des services qui ne sont pas spécifiquement identifiés (p. ex., la navigation générale sur Internet) ira directement sur Internet, en contournant la solution de SSI.

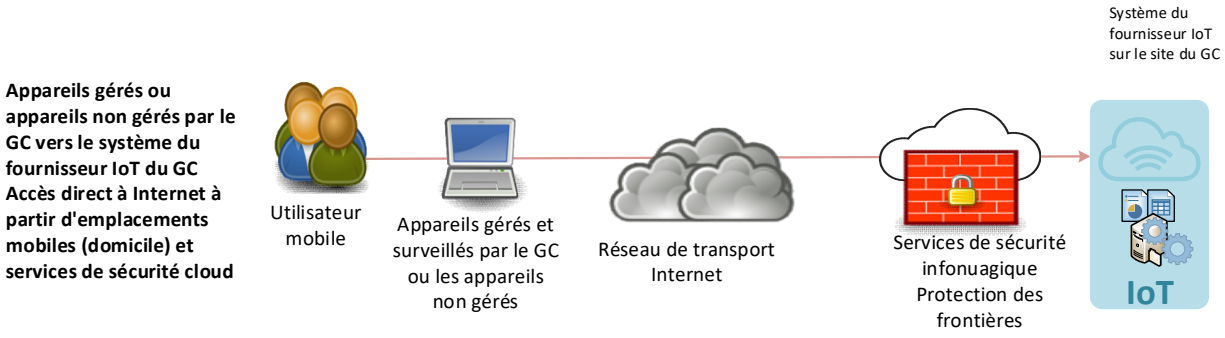
Cas d'utilisation 3b : Utilisateur qui accède à des services sur place du GC (CDE) à l'aide de son propre appareil

Un utilisateur mobile du GC utilise son propre appareil, sans pouvoir installer un logiciel de SSI, pour accéder aux services sur place du GC de l'extérieur des bureaux du GC (à la maison, à l'hôtel, par l'entremise d'une connexion Internet publique, etc.) protégé par des services de sécurité au sein de la solution de SSI. Tout le trafic de l'utilisateur passe par un tunnel chiffré sécurisé depuis le point d'extrémité de l'utilisateur vers la solution de SSI, puis vers la destination dans un CDE du GC.



4. Cas d'utilisation 4a : Accès des utilisateurs aux appareils de l'IO/scientifiques via Internet

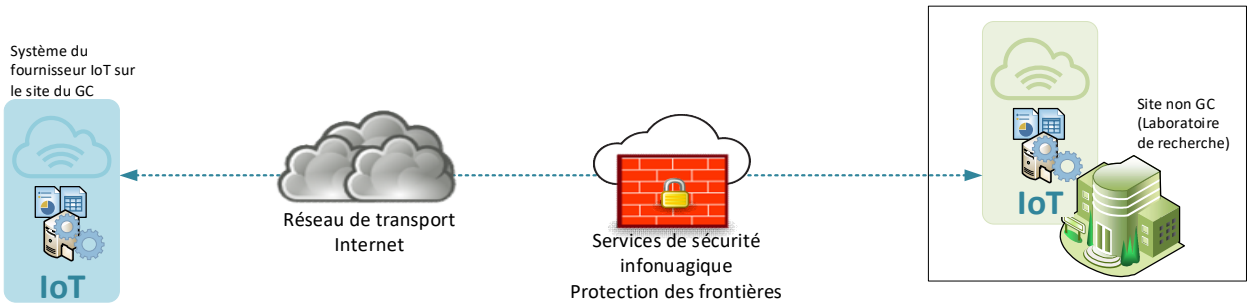
Un appareil de l'IO, tel qu'un capteur, un robot ou un autre appareil scientifique qui réside au sein du GC, peut devoir être accessible ou contrôlé par un utilisateur du GC ou un utilisateur externe via Internet. Le trafic circulerait entre les appareils des utilisateurs et l'IO ou l'appareil scientifique via la solution de SSI.



Cas d'utilisation 4b : Les appareils de l'IO/scientifiques accèdent à d'autres appareils ou systèmes de l'IO/scientifiques via Internet

Un appareil de l'IO, tel qu'un capteur, un robot ou un autre appareil scientifique qui réside au sein du GC, peut avoir besoin de communiquer avec d'autres appareils ou systèmes de l'IO qui résident à l'extérieur du GC (par exemple avec un laboratoire de recherche de l'extérieur du GC ou avec le système d'un fournisseur de l'IO) via Internet. Le trafic circulerait entre l'IO ou les appareils et systèmes scientifiques via la solution de SSI.

L'accès aux appareils et entre eux serait autorisé ou refusé par la solution de SSI.

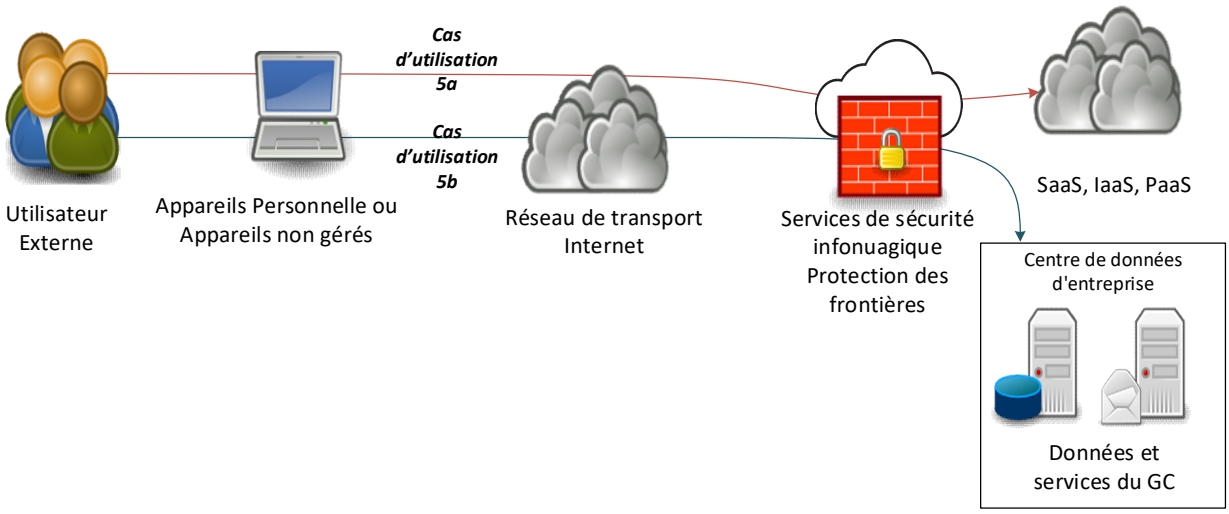


5. **Cas d'utilisation 5a : Utilisateur externe qui utilise un appareil non géré par le GC ou son propre appareil pour accéder aux services infonuagiques du GC**

Un utilisateur externe utilise un appareil non géré par le GC ou son propre appareil pour accéder aux applications, données ou services infonuagiques du GC (p. ex., SaaS, IaaS, PaaS) de l'extérieur du GC. L'accès serait autorisé ou refusé par la solution de SSI.

Cas d'utilisation 5b : Utilisateur externe qui utilise un appareil non géré par le GC ou son propre appareil pour accéder aux services sur place (CDE) du GC

Un utilisateur externe utilise un appareil non géré par le GC ou son propre appareil pour accéder aux applications, aux données ou aux services sur place du GC dans un CDE du GC de l'extérieur du GC. L'accès serait autorisé ou refusé par la solution de SSI.

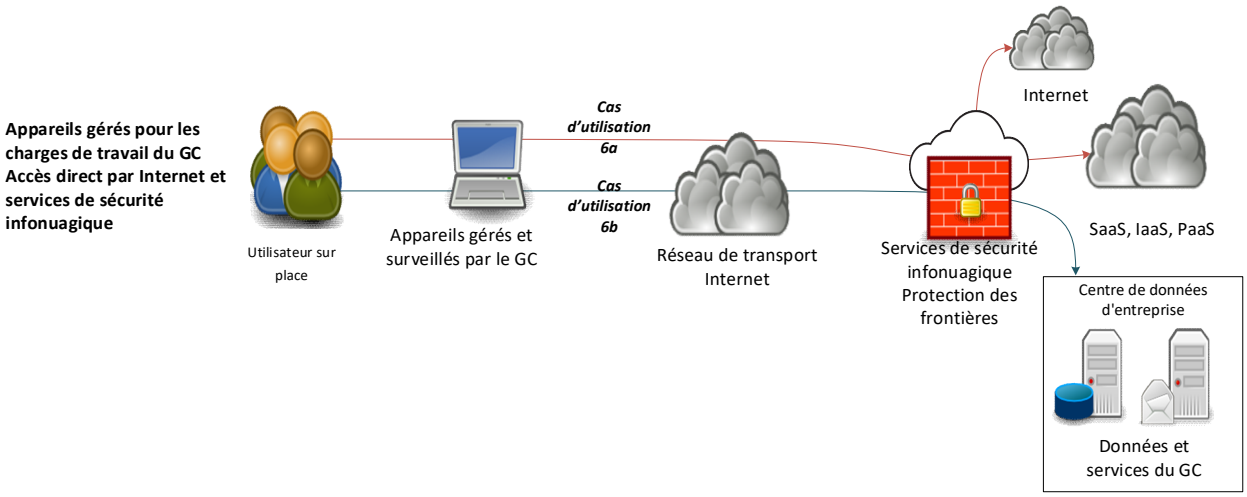


6. **Cas d'utilisation 6a : Utilisateur (appareil géré) situé sur un site éloigné du GC qui accède aux services infonuagiques**

Un utilisateur du GC muni d'un appareil géré accède aux services infonuagiques par l'intermédiaire d'une connexion Internet directe du site éloigné du GC, protégé par les services de sécurité de la solution de SSI. Tout le trafic de l'utilisateur passe par un tunnel chiffré sécurisé vers la solution de SSI.

Cas d'utilisation 6b : Utilisateur (appareil géré) situé sur un site éloigné du GC qui accède aux services sur place (CDE) du GC

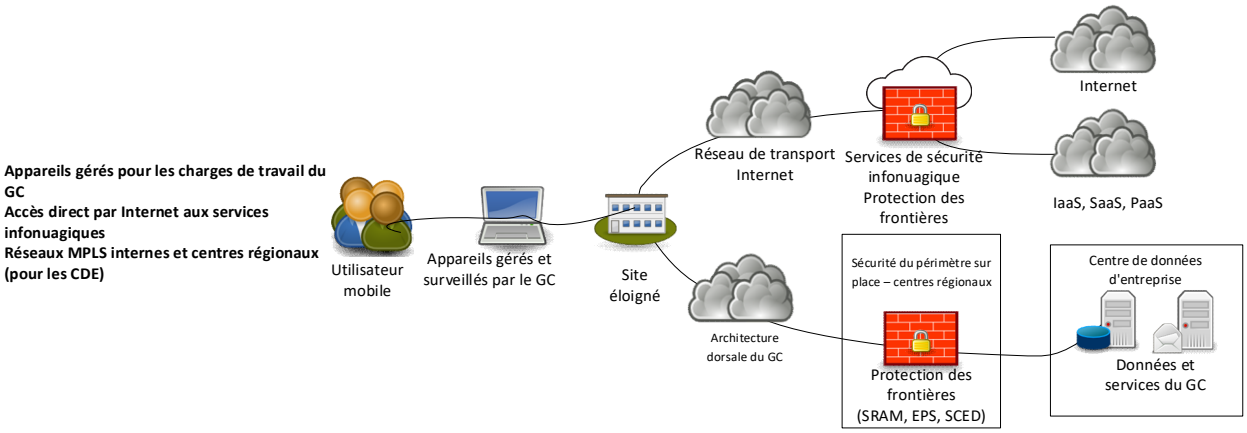
Un utilisateur du GC muni d'un appareil géré accède aux services sur place du GC situés dans un CDE du GC par l'intermédiaire d'une connexion Internet directe du site éloigné du GC, protégé par les services de sécurité de la solution de SSI. Tout le trafic de l'utilisateur passe par un tunnel chiffré sécurisé vers la solution de SSI.



7. Cas d'utilisation 7 : Utilisateur situé sur un site éloigné du GC et muni d'un appareil géré qui accède aux services infonuagiques par l'intermédiaire d'une connexion Internet, et aux services sur place du GC (CDE) par l'intermédiaire d'un centre régional.

Un utilisateur situé sur un site éloigné et muni d'un appareil géré accède aux services infonuagiques par l'intermédiaire d'une connexion Internet directe. Une partie du trafic de l'utilisateur passe par un tunnel chiffré sécurisé de l'utilisateur vers la solution de SSI, puis vers la destination dans le nuage public (p. ex., accès général à Internet, SaaS, IaaS ou PaaS).

L'utilisateur accède également aux services sur place du GC (CDE) par un circuit MPLS dorsal reliant le site éloigné du GC et un centre régional. Tout le trafic entre les services sur place du GC (CDE) et l'utilisateur passe par le centre régional.



Exigences minimales viables obligatoires

Les sections suivantes décrivent les capacités minimales escomptées de la solution. On y présente, entre autres :

- les exigences fonctionnelles : ce que la solution doit faire (tout le temps) et doit pouvoir faire lorsqu'elle y est invitée; et
- les exigences non fonctionnelles : comment la solution doit interagir avec l'environnement et les autres appareils.

1. Capacités (CAP)

CAP1 : La solution doit fournir un accès général à Internet et un accès aux services infonuagiques IaaS, PaaS et SaaS aux utilisateurs mobiles approuvés qui se connectent via une connexion Internet directe en utilisant :

a) un appareil géré par le GC;
b) un appareil non géré par GC.

CAP2 : La solution doit fournir un accès aux services infonuagiques IaaS, PaaS et SaaS aux utilisateurs mobiles approuvés qui se connectent via une connexion Internet directe à l'aide de leur propre appareil.

CAP3 : La solution doit fournir un accès aux applications, aux données et aux services Web du GC sur place aux utilisateurs qui se connectent via une connexion Internet directe à l'aide de leur propre appareil.

CAP4 : La solution doit fournir un accès général à Internet et aux services infonuagiques IaaS, PaaS et SaaS aux utilisateurs autorisés situés sur des sites éloignés du GC qui utilisent une connexion Internet publique directe à partir d'un appareil géré par le GC.

CAP5 : La solution doit fournir un accès aux applications, aux données et aux services sur place du GC aux utilisateurs autorisés situés sur des sites éloignés du GC qui utilisent une connexion Internet publique directe à partir d'un appareil géré par le GC.

CAP6 : La solution doit permettre aux administrateurs autorisés de configurer les politiques d'accès des utilisateurs, des groupes et des appareils pour :

a) Autoriser ou refuser l'accès d'un utilisateur, d'un groupe ou d'un appareil aux services, quel que soit l'endroit où ils sont hébergés, en fonction des politiques d'accès configurées par le GC et par les différents ministères et organismes du GC;
b) Limiter l'accès aux services, quel que soit l'endroit où ils sont hébergés, aux services qui ont été explicitement autorisés, tel que définis dans les politiques d'accès créées par le GC et les différents ministères et organismes du GC;
c) Refuser tout accès et toute visibilité à tous les services auxquels un utilisateur, un groupe ou un appareil n'est pas explicitement autorisé à accéder.

CAP7 : La solution doit fournir les capacités d'expérience utilisateur suivantes pour les appareils gérés et non gérés par le GC :

a) surveillance continue de la performance de l'expérience utilisateur;
b) fournir un score de l'expérience utilisateur au fil du temps, ce score étant utilisé pour déterminer le niveau de l'expérience utilisateur (p. ex., expérience utilisateur médiocre, acceptable, excellente) et les tendances de l'expérience utilisateur;
c) fournir des rapports sur l'expérience utilisateur;
d) alerter les administrateurs lorsque le score de l'expérience utilisateur tombe en dessous d'un seuil prédéfini;
e) permettre aux administrateurs de déterminer où et pourquoi un utilisateur est confronté à une mauvaise performance.

CAP8 : La solution doit pouvoir désactiver automatiquement l'agent de la solution de SSI lorsqu'un utilisateur se trouve dans un bureau physique du GC.

CAP9 : La solution doit pouvoir empêcher les utilisateurs finaux de se déconnecter ou de désactiver l'agent de la solution de SSI afin d'éviter qu'ils contournent la solution.

CAP10 : La solution doit permettre aux administrateurs autorisés de sélectionner le site du centre de données régional de la solution de SSI vers lequel le trafic des utilisateurs est acheminé.

CAP11 : La solution doit fournir un accès aux applications, aux données et aux services du GC sur place, lorsqu'il existe des adresses IP qui se chevauchent ou en double.

CAP12 : La solution doit permettre l'accès direct aux applications de confiance, telles que définies par le Canada, en contournant la solution de SSI.

CAP13 : La solution de SSI ne doit pas nécessiter l'utilisation de plus d'un agent de la solution de SSI sur un appareil d'utilisateur final quelconque.

CAP14 : La solution doit permettre aux utilisateurs externes d'accéder aux appareils de l'IO et scientifiques sur place du GC.

CAP15 : La solution doit fournir un accès aux appareils de l'IO et scientifiques sur place du GC pour communiquer et transmettre des données à d'autres appareils et systèmes de l'IO et scientifiques autres que ceux du GC situés à l'extérieur du GC (p. ex., les systèmes des FEO de l'IO, les laboratoires de recherche externes).

CAP16 : La solution doit prendre en charge la traduction d'adresse réseau (TAR).

2. Securité (SEC)

SEC1 – La solution doit chiffrer toutes les données en transit tout en :

a) établissant des connexions sécurisées aux services infonuagiques, notamment en assurant la protection des données en transit entre le Canada et le service infonuagique au moyen du protocole TLS 1.2 ou de versions ultérieures;
b) utilisant des protocoles ainsi que des algorithmes et des certificats cryptographiques pris en charge et à jour, comme le décrivent les normes ITSP.40.062 (https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062) et ITSP.40.111 (https://cyber.gc.ca/fr/orientation/algorithmes-

cryptographiques-pour-linformation-non-classifie-protege-et-protege-b) du Centre de la sécurité des télécommunications (CST);

c) utilisant une longueur de clé ECDSA d'au moins 256 octets;
d) utilisant une longueur de clé RSA d'au moins 2 048 octets.

SEC2 : La solution doit pouvoir utiliser des clés de l'ICP du GC émises par une autorité de certification du GC pour protéger l'accès aux applications, aux données et aux services hébergés par le GC.

SEC3 – La solution doit pouvoir authentifier les utilisateurs en utilisant les méthodes d'authentification Web suivantes :

a) fédération à l'aide du langage de balisage des assertions de sécurité (SAML) 2,0, dans lequel les justificatifs d'identité de l'utilisateur final et l'authentification pour les services infonuagiques se trouvent dans un fournisseur d'identité (FI) qui est contrôlé exclusivement par le Canada;
b) la mise en œuvre de l'ADFS par le GC à l'aide du protocole SAML 2.0.

3. Capacités de sécurité (CAPS)

CAPS5 – La solution doit fournir les services infonuagiques de sécurité du périmètre suivants :

a) un pare-feu de couche 4 à 7 qui autorise ou refuse l'accès en fonction des adresses IP, des ports, des protocoles, de l'application, de l'identité, des groupes et des emplacements (c'est-à-dire un pare-feu de nouvelle génération (NGFW);
b) filtrer les logiciels/logiciels malveillants indésirables du trafic Internet déclenché par l'utilisateur, appliquer la conformité aux politiques pour le trafic Web et empêcher l'accès aux sites Web inacceptables/illégaux et aux sites Web connus pour contenir des logiciels malveillants ou des virus (c'est-à-dire la passerelle Web sécurisée (SWG);
c) analyser le trafic déchiffré et normal pour détecter les tentatives d'intrusion et les bloquer (c'est-à-dire un système de détection et de prévention d'intrusion (IDPS));
d) reconnaître et bloquer les logiciels malveillants intégrés dans les fichiers en transit et les fichiers contenant des logiciels malveillants, et assurer ainsi une protection contre les menaces actuelles et nouvelles. La solution évalue et détermine les menaces avancées progressives et hautement sophistiquées en inspectant le contenu des fichiers applicables (c'est-à-dire la détection avancée des menaces [ATD]);
e) déchiffrer et inspecter le trafic SSL et TLS pour détecter les menaces, en protégeant SPC contre les tentatives d'utilisation de code malveillant caché dans les flux de trafic chiffrés (c'est-à-dire l'inspection de la couche de sockets sécurisés/du protocole de sécurité de la couche transport [SSL/TLS]);
f) reconnaître les transferts de fichiers au moyen des protocoles SCP ou SFTP qui doivent être inspectés par d'autres services de sécurité, tels que l'ATD (c'est-à-dire l'inspection SSH).

CAPS2 : La solution doit pouvoir bloquer automatiquement tous les fichiers qui ont été identifiés comme étant malveillants pour tous les locataires.

CAPS3 : La solution doit permettre de mettre en quarantaine les fichiers dont il a été déterminé qu'ils étaient malveillants et de les mettre à la disposition du GC pour une enquête plus approfondie.

CAPS4 : La solution doit reconnaître et pouvoir contrôler les applications Web indépendamment du port ou du protocole.

CAPS5 : La solution doit pouvoir identifier le système d'exploitation et l'agent de navigation de l'utilisateur et retracer les activités jusqu'aux différents utilisateurs.

CAPS6 : La solution doit faire le suivi de toutes les modifications administratives et les consigner. Les journaux des modifications doivent :

a) contenir l'heure, la date, le nom d'utilisateur de l'administrateur et les détails de la modification;
b) être entreposés dans un endroit sécurisé;
c) être protégés pour assurer et prouver qu'ils n'ont pas été modifiés ou altérés (c'est-à-dire la non-répudiation).

CAPS7 : La solution doit transmettre les journaux à plusieurs systèmes de GIES du GC.

CAPS8 : La solution doit fournir des évaluations de l'état des dispositifs de sécurité pour les appareils gérés et non gérés par le GC afin d'autoriser ou de refuser les privilèges d'accès aux applications, aux données et aux services.

4. Authentification (AUTH)

AUTH1 : La solution doit pouvoir prendre en charge les méthodes d'authentification du GC suivantes :

a) authentifier les appareils à l'aide de certificats émis par le GC;
b) procéder à l'authentification et à l'autorisation des utilisateurs stockés dans les répertoires du GC accessibles par l'entremise de la LDAPS;
c) autoriser les utilisateurs via une combinaison de groupes d'utilisateurs et d'attributs d'utilisateur;
d) authentifier les appareils et les utilisateurs qui prennent en charge l'IU.

AUTH2 : La solution doit pouvoir utiliser les méthodes d'authentification multifacteurs (AMF) suivantes :

a) appareil OTP multifacteurs;
b) jeton logiciel sur un appareil portable;
c) notification poussée multifacteurs sur un appareil mobile;
d) certificat d'utilisateur des ICP du GC;
e) cartes intelligentes.

AUTH3 : La solution doit pouvoir forcer les administrateurs de la solution SSI à utiliser une solution d'authentification à deux facteurs (A2F) fournie par le GC.

6. Connectivité (CON)

CON1 – La solution doit assurer une expérience utilisateur des services infonuagiques d'excellente qualité en :

a) assurant un appairage direct avec les fournisseurs de services infonuagiques et les fournisseurs d'échange Internet; ou

b) tirer parti de la mise en réseau des fournisseurs de services infonuagiques sous-jacents qui hébergent la solution de SSI.

7. Interopérabilité (IOP)

IOP1 – La solution doit fonctionner sur les systèmes d'exploitation suivants :

a) famille de systèmes d'exploitation Windows pris en charge par Microsoft;
b) famille de systèmes d'exploitation macOS et iOS pris en charge par Apple;
c) système d'exploitation Android pris en charge par Google;
d) système d'exploitation Linux soutenu commercialement et par la communauté.

IOP2 : La solution doit prendre en charge l'accès Web à partir des navigateurs Web suivants : Apple Safari, Microsoft Edge, Google Chrome et Mozilla Firefox.

8. Intégration (INT)

INT1 : La solution doit s'intégrer aux solutions SOAR du GC à l'aide du transfert d'état représentationnel (REST).

INT2a : La solution doit fonctionner avec l'agent CASB d'un autre fournisseur installé sur l'appareil d'un utilisateur final.

INT 2b : L'agent CASB de la solution et l'agent CASB de l'autre fournisseur doivent fonctionner ensemble et diriger le trafic tel que défini par le Canada.

INT3a : La solution doit fonctionner avec un agent RPV d'un autre fournisseur installé sur l'appareil d'un utilisateur final.

INT3b : L'agent de la solution et l'agent RPV de l'autre fournisseur doivent fonctionner ensemble et diriger le trafic tel que défini par le Canada.

INT4 : La solution doit appliquer les approches à vérification systématique suivantes :

a) l'évaluation et l'autorisation continues des demandes d'identité et d'accès des utilisateurs;
b) l'application d'une politique fondée sur des profils d'utilisateurs récupérés dans un ou plusieurs dépôts d'identité du GC;
c) les utilisateurs ont accès aux applications, aux données et aux services en fonction de l'identité, de la géolocalisation, de l'authentification de l'appareil et de l'évaluation de la posture, ainsi que des entrées contextuelles des autres utilisateurs et appareils.

9. Gestionnaires (GEST)

GEST1 : La solution doit prendre en charge la multilocation et permettre ainsi à plusieurs administrateurs du GC de différentes organisations d'assurer la gestion, de générer des rapports personnalisés et d'administrer des parties spécifiques de la solution dans leur domaine autorisé.

GEST2 : La solution doit pouvoir appliquer le contrôle de l'accès en fonction des rôles granulaire aux utilisateurs administrateurs.

GEST3 : La solution doit prendre en charge les organisations d'opérateurs multilocataires par le biais d'un contrôle d'accès en fonction des rôles hiérarchique, dans lequel les organisations de niveau supérieur (parents) ont une visibilité et un contrôle complets sur toutes les organisations et politiques subordonnées (enfants).

GEST4 : La solution doit permettre au GC de mettre en œuvre des politiques globales qui s'appliquent aux locataires et qui ne peuvent pas être modifiées ou supprimées par les administrateurs de l'organisation enfant.

GEST5 : La solution doit restreindre la capacité des organisations enfants à modifier la politique ou le comportement de la solution pour toute autre organisation, y compris l'organisation parent.

GEST6 : La solution doit permettre de :

a) générer des rapports ponctuels personnalisés fondés sur les rôles;
b) envoyer des journaux propres aux locataires au ministère locataire.

10. Déploiement et environnement opérationnel (ENV)

ENV1 : La solution doit pouvoir être déployée dans une configuration qui fait en sorte que les points d'extrémité des appareils sont en mesure de se connecter à la solution en cas de panne de l'équipement ou du site.

ENV2 : La solution doit pouvoir prendre en charge un minimum de 100 000 utilisateurs simultanés.

Exigences non obligatoires

Cas d'utilisation non obligatoire : connexions de serveur à serveur dans un environnement infonuagique IaaS

Une charge de travail du GC sur un serveur dans un environnement IaaS (p. ex., Azure Web Services, Azure, Google Cloud Platform, etc.) se connecte à un autre serveur ou à une autre charge de travail du GC dans un environnement IaaS différent, de façon protégée par les services de sécurité de la solution de SSI. L'accès à ces services est fondé sur des politiques.

ENO1 : La solution doit fournir le type d'accès sécurisé suivant entre les serveurs dans un environnement infonuagique IaaS :

a) des communications de serveur à serveur entre les fournisseurs de services infonuagiques IaaS (p. ex., entre Azure Web Services et Azure);
b) des communications interrégionales de serveur à serveur, au sein d'un même fournisseur de services infonuagiques (p. ex., entre un serveur de la région 1 et un serveur de la région 2).

ENO2 : Soutien pour les utilisateurs internationaux – La solution doit connecter les utilisateurs du GC et les utilisateurs externes situés physiquement à l'extérieur du Canada directement aux centres de données de la solution de SSI situés au Canada et aux centres de données de la solution de SSI approuvés par le GC situés à l'extérieur du Canada.

ENO3 : Gestion de la posture de sécurité du nuage (CSPM) – La solution doit avoir une fonctionnalité CSPM native qui :

a) surveille, détermine et évalue la conformité à la sécurité et les violations réglementaires dans les environnements IaaS et PaaS;
b) avise les administrateurs et fournit des rapports sur la non-conformité à la politique de sécurité, les erreurs de configuration et les violations de la réglementation;
c) automatise la correction des non-conformités aux politiques de sécurité, des erreurs de configuration et des violations de la réglementation détectées.

ENO4 : Gestion de la posture de sécurité SaaS (SSPM) – La solution doit posséder une capacité SSPM native qui surveille et détecte les paramètres qui créent des risques pour la sécurité dans l'environnement SaaS, fournit des alertes en cas de mauvaise configuration et automatise ou fournit une correction guidée pour résoudre les risques.

ENO5a : Isolement de navigateur à distance (RBI) – La solution doit posséder une capacité RBI native qui permet à l'activité de navigation Web d'un utilisateur d'être exécutée sur un serveur éloigné dans un environnement isolé, plutôt que sur l'ordinateur de l'utilisateur.

ENO5b : La capacité RBI native de la solution doit être hébergée dans l'environnement infonuagique du FEO de la solution de SSI.

ENO5c : La capacité RBI native de la solution doit protéger les ordinateurs des utilisateurs des menaces Web en contenant les menaces dans l'environnement isolé.

ENO5d : La capacité RBI native de la solution doit autoriser et refuser :

a) les téléverments de fichiers;
b) les téléchargements de fichiers;
c) les captures d'écran;
d) le copier et coller de toute information affichée.

ENO6 : Courtier natif de la sécurité de l'accès du nuage (CASB) – La solution doit posséder une capacité CASB native et intégrée qui comprend au moins la prévention de la perte de données (PPD), l'analyse du comportement des utilisateurs et des entités (UEBA), la conformité à la réglementation et aux politiques et la détection des menaces.

ENO7 : SD-WAN – La solution doit posséder une capacité SD-WAN native et intégrée.

ENO8 : Découverte d'applications automatisée – La solution doit découvrir et identifier automatiquement les applications auxquelles accèdent les utilisateurs ou appareils de la solution de SSI et permettre ainsi aux administrateurs de la solution de SSI d'appliquer facilement les politiques d'accès des utilisateurs à ces applications.

ENO9 : Analyse du comportement des utilisateurs et des entités (UEBA) – La solution doit détecter et signaler les comportements suspects des utilisateurs et des appareils.

ENO10 : La solution doit accomplir des actions automatisées pour bloquer les menaces potentielles en fonction du comportement qui a été identifié comme étant un risque ou une menace potentielle. Par exemple, si la solution détecte qu'un utilisateur a un comportement suspect, elle lui refuse automatiquement l'accès, le met en quarantaine (ainsi que l'appareil, le cas échéant) et signale le tout à un administrateur.

ENO11 : Intégration de la sécurité du point d'extrémité – La solution doit pouvoir s'intégrer aux logiciels de sécurité des points d'extrémité pris en charge par le GC, tels que McAfee, Windows Defender et Cisco AMP for Endpoints pour :

a) automatiser les réponses aux menaces qui ont été détectées par la solution de sécurité des points d'extrémité;
b) fournir de l'information sur les menaces qui ont été détectées par la solution de SSI à la solution de sécurité des points d'extrémité, afin que la solution de sécurité des points d'extrémité puisse automatiser une réponse à la menace détectée.

ENO12 : Déploiement de la solution de SSI du GC sur place – La solution doit permettre de déployer une instance de la solution de SSI dans un centre de données du GC. Une seule instance de la plateforme de gestion infonuagique centralisée de la solution de SSI doit gérer à la fois le déploiement de la solution SSI sur place et l'environnement infonuagique de la solution de SSI.

ENO13 : La solution doit permettre un appairage direct avec les fournisseurs d'échange Internet à un minimum de 100 Gb/s.

ENO14 : La solution doit pouvoir procéder à l'authentification et à l'autorisation avec Open Authorization version 2 et avec OpenID (OAuth v2.0).

ENO15 : La solution doit fournir un accès sécurisé aux applications, aux données et aux services du GC sur place non basés sur le Web pour les utilisateurs mobiles qui utilisent leur propre appareil par l'entremise de RDP, de SSH et du montage de système de fichiers à distance (p. ex., SMB).

ENO16 : La solution doit fournir de l'information sur la qualité des appels et des rapports pour les appels Microsoft Teams, y compris des analyses du réseau (p. ex., la latence).

ENO17 : La solution doit pouvoir distinguer les versions approuvées et non approuvées par le GC et les versions personnelles des applications d'infonuagique publique et être capable de prendre des décisions relativement à la politique d'accès associées à un utilisateur en fonction de l'appareil qu'il utilise. Par exemple, sur un appareil géré par le GC, les applications d'infonuagique d'entreprise seront autorisées mais les versions personnelles doivent être bloquées.

ENO18 : La solution doit accomplir des fonctions de prévention de la perte de données (PPD) qui comprennent, au minimum :

a) politiques de conformité prédéfinies de l'industrie (renseignements permettant d'identifier une personne du Canada, PCI-DSS);
b) identificateurs de données canadiens intégrés spécifiques (carte Santé, permis de conduire);
c) identifiants personnalisés des données;
d) prise en charge de l'expression régulière (RegEx);
e) modèles personnalisés et correspondance exacte des données;
f) possibilité de créer des règles et des profils de PPD personnalisés;
g) inspection des fichiers zip;
h) inspection des champs cachés;
i) détection des fichiers chiffrés.

ENO19 : La solution doit posséder des capacités d'application Web et de protection de l'ARP en tant que service (WAAPaaS).

ENO20 : La solution doit s'intégrer aux solutions SOAR du GC à l'aide du langage de balisage extensible (XML).

ENO21 : La solution doit fournir les capacités d'expérience utilisateur suivantes pour les appareils gérés et non gérés par le GC :

a) fournir des mesures de la latence saut par saut, en indiquant la latence de tous les sauts, du point d'extrémité de l'utilisateur à la destination;
b) déterminer la disponibilité des applications publiques et privées de destination et le temps de réponse pour aider à déterminer si l'application est responsable de la mauvaise qualité de l'expérience utilisateur;
c) inclure des mesures de la performance pour l'appareil de l'utilisateur final, y compris des statistiques sur le processeur, la mémoire et le Wi-Fi.

ENO22 : La solution doit fournir un accès aux appareils de l'IO et scientifiques du GC situés à l'extérieur d'un site du GC pour communiquer et transmettre des données à d'autres appareils et systèmes de l'IO et scientifiques situés à l'extérieur des sites du GC (systèmes de l'IO des FEO vers des laboratoires de recherche externes).

ENO23 : La solution doit effectuer l'authentification et l'autorisation pour les utilisateurs à l'aide d'un dépôt d'identités situé dans la solution de SSI rempli à l'externe à partir de sources faisant autorité du GC.

ENO24 : La solution doit authentifier et autoriser l'appareil de l'utilisateur final avant d'autoriser l'accès aux applications, aux données et aux services.

ENO25 : La solution doit pouvoir prendre en charge un minimum de 100 000 utilisateurs simultanés.

ENO26 : La solution doit être capable d'implémenter un capteur basé sur réseau virtuel du GC permettant la capture des données sélectives du GC et de transmettre ces données à divers sites du GC pour des analyses plus approfondies.

Personas

Nom

Dr Abigail

Utilisateurs n'appartenant pas au GC qui ont besoin d'accéder aux données du GC (p. ex., les établissements d'enseignement)

Données démographiques : Sciences

- Chercheur dans une université (pourrait être un expert en la matière)
- Pourrait être en train d'achever une maîtrise ou un doctorat ou possède déjà un doctorat

Objectifs	**Défis**
• Scientifiques ayant besoin d'accéder à des capacités de calcul de haute performance (CHP) pour exécuter des algorithmes. • Transfert facile et rapide de grandes quantités de données (téraoctets) sur la grappe et hors de celle-ci; rapidité est synonyme de productivité. • Accès facile à des sites particuliers : Calcul Canada, Dépôt fédéré de données de recherche (FRDR) ou autres. • Généralement, le trafic n'est pas en temps réel. • Certains pourraient utiliser la diffusion en continu du trafic. • Possibilité d'avoir un accès à la volée (c'est-à-dire dans les 24 heures ou moins). • Accès aux équipements et contrôle de ceux-ci (p. ex., les robots dans les laboratoires gouvernementaux); toujours de grandes quantités de données sous forme de vidéos haute définition ou d'appareils scientifiques/non humains/Internet des objets (p. ex., des capteurs qui transmettent des données en continu). L'automatisation doit permettre de conserver les données dans l'installation pour qu'elles y soient analysées.	• Certaines personnes utilisent un environnement Linux; nécessité de prendre en charge plusieurs systèmes d'exploitation. • Outils de sécurité – susceptibles de réduire la vitesse. • Mauvaise expérience utilisateur – latence élevée. • Politiques de sécurité – comment gérer l'identité et l'authentification? • Les utilisateurs et scientifiques ne peuvent pas installer de logiciels sur leurs ordinateurs. • Tous les types d'accès ne sont pas liés à un navigateur Web ou à une API. • Accès depuis l'extérieur du Canada (exigence relative à un accès mondial).
Valeurs	**Craintes**
• La connexion est simple (l'authentification à deux facteurs est parfois ignorée). • Le mode d'accès sera similaire à celui d'autres systèmes que les utilisateurs connaissent déjà.	• Sauts supplémentaires – susceptible de perturber le trafic et de le ralentir. • Peur de perdre l'accès – fiabilité et pannes. • Certaines recherches portent sur des données sensibles.

Attentes	**Mesures du succès**
• Une fois l'accès accordé, si la performance est bonne, elle le restera. • Une fois que le système est opérationnel, la manière dont les autorisations sont accordées est faite par les chercheurs (dans le cadre du contrôle de leur service), c'est-à-dire que l'accès est basé sur le rôle et que les autorisations sont accordées selon le système (contrôle de l'accès en fonction des rôles ou RBAC). • Les utilisateurs obtiennent uniquement l'accès aux systèmes auxquels ils ont besoin d'avoir accès et les autorisations pour les projets auxquels ils ont accès. • Délai de traitement de 24 heures (pour le processus d'accueil et de départ des collaborateurs). • L'aspect et la convivialité sont similaires à ceux auxquels les utilisateurs sont habitués. • Nécessité d'une haute disponibilité. • Système de soumissions de billets pour soutenir les utilisateurs externes – modèle de soutien aux scientifiques pour une résolution rapide (gestion des services de TI ou GSTI).	1. Connexion rapide et flexible pour le déplacement des données (vitesse). 2. Expérience utilisateur – transparente et simple. 3. L'utilisateur se connecte une seule fois et accède à ce dont il a besoin – simplicité d'utilisation. • Aucun besoin d'installer de nouveaux logiciels. • Système de secours.

Nom

Pénélope

ISO/SOC

Données démographiques :

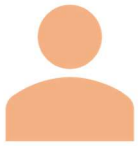
- CS2 à CS4, à la fois pour ISO et SOC

Objectifs • S'assurer que la technologie et l'infrastructure des solutions infonuagiques sont bien entretenues. • Réponse aux incidents – augmenter les capacités de réponse aux incidents. • Gestion de l'accès (s'assurer que les bonnes personnes disposent des bons privilèges).	**Défis** • Personnel pour gérer la solution. • Qualité des données – enregistrement inadéquat des données. • Volume de données – augmentation du volume de données et dédoublement si elles ne sont pas étiquetées correctement. • Trouver les bonnes personnes pour faire le travail – difficile de trouver des personnes bilingues certifiées SOC (requalification des ressources et formation).
Valeurs • Avoir une meilleure visibilité. • Gérer les connexions Internet disparates (non contrôlées et non sécurisées). • Améliorer la sécurité.	**Craintes** • Double emploi avec d'autres services qui pourraient être en mesure de fournir une solution différente, comparable à la solution de SSBI. • En multipliant les options, on crée plus de complexité, et les risques augmentent. • Comment pouvons-nous garantir l'intégrité des services (afin qu'ils n'aient pas été altérés)? Nous ne gérons pas le contrôle de la sécurité et la façon dont il évoluera dans le temps, ni la gestion des vulnérabilités. • Les partenaires contournent la sécurité de SPC pour prendre le contrôle de leur domaine. Des protections seront-elles mises en place pour éviter les erreurs?
Attentes • Ce serait bien d'avoir un endroit centralisé pour gérer les locataires (p. ex., afin de pouvoir accéder à tous les locataires au moyen d'un cyberévénement); si quelque chose doit être remplacé partout, à quelle vitesse pouvons-nous les joindre? (locataires de SPC, de l'Agence du revenu du Canada, etc.) – cartographie centralisée – observabilité. • Une politique globale peut avoir une incidence sur chaque organisation partenaire; politique propre à chaque ministère (multilocation parent/enfant). • Intégration avec d'autres services de sécurité pour la surveillance, l'observabilité et la visibilité. • Préparation des données afin de résoudre les problèmes de qualité et de volume (de sorte que les données soient cohérentes lorsqu'elles sont corrélées). • Maintien et suivi de l'adresse IP source. • Possibilité de copier ou d'appliquer les paramètres à tous les locataires.	**Mesures du succès** 1. Vue d'ensemble de l'infrastructure. 2. Renseignements utiles – intégration, facilitée d'accès – télémétrie exploitable (ne pas créer plus de travail) – la solution nous indique où chercher. 3. Réduction des efforts de triage des incidents. 4. Amélioration de la posture de sécurité, c'est-à-dire que la tunnellisation divisée peut exposer une partie de l'infrastructure (p. ex., lorsque le trafic ne passe pas par le RPV). • Conservation des données enregistrées *(intégrité des journaux, tous les journaux sont envoyés, ils ne sont pas perdus).* • Architecture appropriée – inclusion de l'authentification à deux facteurs dans le RBAC. • Convivialité – interface utilisateur graphique facile à utiliser; nul besoin de faire appel à des services professionnels; pas besoin de script. • Demande globale de location.

• Matrice RACI bien architecturée s'il s'agit d'un modèle fédéré – la responsabilité du changement doit être en place. • Gestion solide du changement (à partir d'une politique globale de référence). • Disponibilité de 99,999 % en tout temps. • Moyen de surveiller l'état de l'environnement – ou l'accès au personnel susceptible de contribuer à résoudre des problèmes de performance et de fiabilité.	• Conformité aux exigences en matière de langue et d'accessibilité.

Nom

Sierra



Administrateurs des ministères et des locataires, et responsables de domaine de spécialité

Données démographiques :

- RE5 à 6, CS4

Objectifs	**Défis**
• Accès aux journaux de bout en bout – échange d'information en temps réel (pour atténuer les incidents), y compris les éléments de SPC. • IdO (appareils non humains) – p. ex., une caméra avec une carte 4G qui effectue des téléversements à tout moment, en tout lieu et sur tout appareil; nous voulons protéger et authentifier ces appareils. • Intégration avec les organisations partenaires, Active Directory et infrastructure à clés publiques (ICP) • Convivialité	• Même si certains événements de sécurité sont gérés par SPC, il est difficile de comprendre et de déterminer ce qui s'est passé. • Quels sont les systèmes en place en ce qui concerne la résidence des données? Les données restent-elles au Canada? • Déchiffrement des données. • Amélioration de la fiabilité des données. • Profil de menace MD5 – disposer de mesures de sécurité supplémentaires.
Valeurs	**Craintes** • Mauvaise performance (expérience utilisateur). • Sans une matrice RACI claire, il se peut que des blâmes soient jetés – chacun doit assumer ses responsabilités (interne au gouvernement).
Attentes • Intégration avec les contrôles de sécurité existants – l'infrastructure de sécurité du périmètre fonctionnerait avec la solution de SSBI. • Flexibilité nécessaire pour pouvoir s'adapter aux besoins des ministères; chaque ministère possède sa propre location. • Les administrateurs ministériels géreraient le ministère (c'est-à-dire que le ministère gère son propre système). • Politique globale pour tous les locataires. • Indicateurs de rendement clé et rapports (à l'intention des cadres) pour présenter le niveau de sécurité aux organisations partenaires sur la base de preuves (c'est-à-dire prouver que les informations sont sécurisées) et les tendances – pour avoir la certitude que les incidents sont traités rapidement. • Pour ceux qui ont des équipes de TI réduites, il faut davantage d'automatisation ou d'apprentissage automatique pour alléger la gestion du système (autant que possible).	**Mesures du succès** 1. Amélioration de la sécurité. 2. Action automatisée pour atténuer les répercussions des incidents. 3. Expérience utilisateur – l'utilisateur final ne sait pas que la solution de SSBI existe; il peut simplement se connecter au besoin, sans avoir à se soucier de la complexité de l'infrastructure réseau. • Intelligence artificielle pour gérer les intrusions et les logiciels malveillants. • Temps de fonctionnement optimal (aucun temps d'arrêt). • Aucune latence – vitesse d'accès à l'information du point de vue de l'utilisateur final. • Sous un angle opérationnel/administratif, le système est automatisé; nul besoin de recourir à des ressources supplémentaires ni de prendre en charge un autre système avec le même nombre de ressources.

Nom

Isabelle

Employés du GC et entrepreneurs – accès à distance

Données démographiques :

- Tout le monde travaille à distance à plein temps
- Provenant de toutes les régions du Canada
- Augmentation significative de l'utilisation des services infonuagiques – en raison du télétravail et de l'adoption croissante de services infonuagiques par le gouvernement du Canada
- Accès à des outils de collaboration, à des outils de bureau et à des outils d'entreprise, ainsi qu'à des outils propres au gouvernement
- Applications spécifiques aux ministères se trouvant sur place et dans le nuage
- Accès aux applications internes du gouvernement du Canada et aux applications infonuagiques
- Accès principalement entre 9 h et 17 h (selon le fuseau horaire respectif des utilisateurs)

Objectifs	**Défis**
• Pouvoir accéder rapidement aux applications. • Disposer d'applications qui s'exécutent rapidement (ne pas attendre 20 secondes après chaque clic). • Éviter des étapes inutiles (p. ex., aucune vérification supplémentaire). • Aspect et convivialité similaires à celles de l'expérience de bureau. • Faire son travail et accomplir ses tâches sans que le réseau ou la connexion pose problème – transparent/invisible • Protection des renseignements personnels et confidentialité	• Capacité (des applications et du réseau) à gérer le télétravail. • Impossible que 12 personnes utilisent leur caméra en même temps. • Performance lors de l'accès aux applications et réactivité de celles-ci (pas aussi rapide qu'au bureau). • Accès parfois difficile à certaines applications (p. ex., Emploi et Développement social Canada [EDSC] et d'autres disposant de politiques plus autoimposées).
Valeurs	**Craintes**
• Maintien par les employés des pratiques de confidentialité et de sécurité. • Capacité de s'acquitter de ses tâches. • Vitesse/réactivité des applications auxquelles il faut accéder. • Productivité (et capacité à faire son travail).	• Congestion (trop de personnes essayant d'accéder au réseau en même temps). • Nouveau confinement (avec des enfants et tout le monde sur le réseau en même temps, etc.). • Problèmes techniques en télétravail, nouvelle solution à adopter ou nouveau processus à suivre (les utilisateurs ne peuvent pas se tourner vers la personne à côté d'eux pour obtenir de l'aide ou demander à quelqu'un de venir les aider). Si les problèmes techniques touchent les outils de collaboration, les utilisateurs se trouvent dans l'impossibilité de demander de l'aide, ce qui conduit à l'isolement. • Perte des travaux réalisés (les applications en réseau ne permettent pas l'enregistrement, les délais d'attente du réseau sont excessifs, tout tombe en panne).

	• Perte de productivité et impossibilité pour les utilisateurs d'accéder à ce dont ils ont besoin (et non-respect des délais).
Attentes • Connexion unique. • Solution d'accès à distance fonctionne réellement. • Invisible – connexion facile sans beaucoup d'étapes. • Connexion sur tous les appareils à notre disposition (p. ex., courriels, MS Teams, etc.). • Assistance en cas de panne (cela ne fonctionne pas et nous ne savons pas pourquoi). • Adoption plus rapide de nouveaux services. • Navigation et accès rapide à Internet.	**Mesures du succès** 1. Réponse rapide des applications auxquelles on accède. 2. Pas de déconnexions ni d'interruptions de service. 3. Convivialité – les utilisateurs n'évitent pas d'avoir recours aux services et ne les détestent pas. • Accès à ce qui est nécessaire quand c'est nécessaire. • Faible nombre de problèmes. • Connexion simple et plutôt rapide (peu d'étapes).

Pièce jointe A1 – Exigences de sécurité nuagique

Informatique nuagique – Exigences de sécurité

(Remarque à l'intention des offrants : en plus des exigences de sécurité décrites dans la section intitulée *Exigences de sécurité* (CBSOS 1.9), une pièce jointe A1 finalisée – Exigences de sécurité infonuagique sera énoncée dans la demande d'offres à commandes finale axée sur les défis.)

L'Offrant doit démontrer qu'il respect les exigences de sécurité sélectionnées dans l'Annexe B – Profil de contrôle infonuagique – du Centre Canadien pour la cybersécurité (CCCS) – Guide sur la catégorisation de la sécurité infonuagique (ITSP.50.103)) (https://www.cyber.gc.ca/en/guidance/guidance- security-categorization-cloud-based-services-itsp50103) pour la portée des services d'Informatique Nuagique fournis par l'offrant.

L'offrant doit s'assurer que les données du Canada, l'infrastructure de l'offrant (y compris l'ensemble des services IaaS, PaaS ou SaaS fournis au Canada) et les lieux de service, sont protégés par des mesures de sécurité appropriées qui sont conformes aux exigences énoncées dans les attestations et rapports d'audit suivants en fournissant par un tier partie indépendant un rapport d'évaluation ou de certification pour chacune des niveaux de services (par exemple : IaaS, PaaS et SaaS) à l'intérieur des services Informatique Nuagique proposés, incluant :

- ISO/IEC 27001:2013 Technologie de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Certification obtenue par un organisme de certification accrédité; et
- ISO/IEC 27017:2015 Technologie de l'information -- Techniques de sécurité -- Code de pratique pour les contrôles de sécurité de l'information basée sur ISO/IEC 27002 pour les services d'Informatique Nuagique réalisé par un organisme de certification accrédité;
- ISO/IEC 27018:2014 Technologie de l'information -- Techniques de sécurité -- Code de pratique pour les protection des informations personnellement identifiables (IPI) dans les nuages publics agissant en tant que processeurs IPI – Certification obtenue par un organisme de certification accrédité; et
- AICPA Service Organization Control (SOC) 2 Type II Audit Report 2 Type II pour les principes de confiance en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité – émis par un expert-comptable indépendant certifié.

Chaque certification ou rapport d'audit soumis doivent :

- Identifier le nom légal de l'entreprise de l'offrant ou du sous-traitant ultérieurement concerné;
- Identifier la date de certification de l'offrant ou du sous-traitant ultérieur et le statut de cette certification;
- Identifier les prestations incluses dans le périmètre du rapport de certification. Si des exclusions sont identifiées ou s'il est nécessaire de séparer une organisation sous-

contractante, le rapporte de cette organisation sous-traitante doit être fourni.

Chaque audit donnera lieu à la production d'un rapport d'audit qui devra être mis à la disposition du Canada. Les certifications doivent être accompagnées de preuves à l'appui telles que le rapport d'évaluation ISO élaboré pour valider la conformité à la certification ISO élaboré pour valider la conformité à la certification ISO et doivent divulguer clairement toute constatation importante de l'auditeur. L'offrant doit remédier rapidement aux problèmes soulevés dans tous rapport d'audit à la satisfaction de l'auditeur.

Chaque rapport d'audit pour SOC 2 Type 2 doit être réalisé dans les 12 mois précèdent ["Date de clôture de l'appel d'offre/ de l'offre'' ou "de la date d'attribution du contrat/de l'offre à commandes" ou "avant que le Canada n'exerce l'Option 1 - Déploiement" ou "avant le segment de travail 2 - Déploiement"]. Une lettre de transition peut être fournie pour démontrer que l'entrepreneur est en cours de renouvellement lorsqu'il y a un écart entre la date du rapport de l'organisme de services et la fin de l'exercice de l'organisme utilisateur (C'est à dire, à la fin de l'exercice civil ou financier).

Informatique nuagique – Évaluation de la sécurité

La conformité sera évaluée et validée par le processus d'évaluation de la sécurité des fournisseurs de services infonuagiques (FSI) du Centre Canadien pour la Cybersécurité (CCCS) (ITSM.50.100) (https://www.cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux), "centralisé" ou conformité sera évaluée et validée par le biais d'un processus départemental d'évaluation locale ''localisée'' avec l'appui du CCCS.

L'offrant doit démontrer qu'il a participé à un processus en réussissant à intégrer, participer et terminer le programme. Ceci inclut de fournir la documentation suivante :

(i) Une copie de la lettre de confirmation qui atteste qu'ils ont intégré le programme;

(ii) Une copie du plus récent rapport d'évaluation complété, fourni par le CCCS; et

(iii) Une copie du rapport sommaire le plus récent fourni par le CCSS.

Pour toute demande d'information en lien avec le programme d'évaluation des Ti du CSP (évalution centralisées), l'offrant doit communiquer avec le service à la clientèle du CCCS (https://cyber.gc.ca/fr/).

L'offrant des services d'Informatique Nuagique a l'obligation continue d'informer le CCCS (évaluations centralisées) ou le Ministère (évaluation locale) lorsqu'il y a des changements importants dans sa prestation des services de sécurité informatique soutenant les services et/travaux de l'offrant.

Obligations de sécurité et de confidentialité

L'ensemble des conditions énoncées dans l'annexe 1 ci-joint Schedule 1 - Obligations de sécurité de niveau 2(jusqu'au niveau Protégé B inclus)pour le SaaS et l'annexe 2 ci-joint Schedule 2 – Obligations en matière de protection des renseignements personnels (sauf sous indication contraire) sont incorporées par référence aux présentes et sont réputées avoir la même force et effet que s'ils étaient énoncés dans leur intégralité dans la présente.