Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Canada

Orientation sur la comptabilisation des sous-processeurs en nuage

Approche des services gérés et des approvisionnements axés sur les résultats

Février 2021

Historique du document

Date	Auteur	Description
Nov. 2020	S. Levac	Rédaction originale à l'appui de la collaboration au Groupe de travail sur l'approvisionnement des services en nuage du GC
Janv. 2021	S. Levac	Approbation par le Groupe de travail sur l'approvisionnement des services en nuage du GC
Févr. 2021	S. Levac	Approbation par le Réseau d'expertise en informatique en nuage et en informatique La rétroaction doit inclure un scénario où le fournisseur passe à l'informatique en nuage en cours de contrat.

Table des matières

Historique du document 2
But 4
Contexte 5
Définitions 6
Différenciation entre le modèle SaaS et les services gérés 9
Évaluation des qualifications en matière de sécurité du service géré 10
Évaluation des qualifications en matière de sécurité des fournisseurs de services d'informatique en nuage 11
Approche pour la comptabilisation de l'informatique en nuage dans les approvisionnements 13
- Planification 13
- Rédaction des exigences 14
- Demande de soumissions 15
- Évaluation 15
- Attribution 15
- Exécution 15
  - Avant le lancement 16
  - Après lancement 16
- Clôture 16

Modification des modèles de service après le lancement 16
Sommaire de l'orientation 17
Appendix A – Template Clauses 18
Appendix B – Sample SRCL and Classification Guide 22
Document history 24

But

De plus en plus de scénarios émergent où les fournisseurs du gouvernement du Canada utilisent des services d'informatique en nuage pour offrir leurs produits et services au GC.

Dans ces scénarios, le GC peut avoir fait l'acquisition de services opérationnels comme l'assurance maladie ou la gestion des biens immobiliers, mais ces services comportent des solutions techniques comme des portails libre-service ou des systèmes de gestion des ressources qui reposent sur des services d'informatique en nuage. Un autre exemple est un processus d'approvisionnement axé sur les résultats où l'on décrit la portée souhaitée des résultats, et où les fournisseurs peuvent proposer un ensemble de services et de produits pour atteindre ces résultats, dont certains peuvent comprendre des services d'informatique en nuage. Il s'agit d'un nombre limité d'exemples pour aider à illustrer des scénarios où le GC ne conclut pas directement de contrat avec un fournisseur de services d'informatique en nuage; le fournisseur doit plutôt utiliser un service d'informatique en nuage pour traiter des données sensibles du GC. Dans chacun de ces scénarios, nous désignons le ou les fournisseurs de services d'informatique en nuage comme sous-processeurs des données du GC. Un fournisseur qui utilise les services d'un autre fournisseur pour traiter ou stocker ses données est également connu comme un risque lié aux fournisseurs de quatrième niveau.

Souvent, il est impossible de savoir si les fournisseurs ou les fournisseurs principaux utilisent un service d'informatique en nuage avant la réception des soumissions ou l'attribution du contrat. Dans le pire des cas, on ne le sait qu'après l'attribution du contrat. Le fait de ne pas tenir compte des services d'informatique en nuage avant l'appel d'offres peut entraîner un retard ou une défaillance du processus d'approvisionnement. Les acquisitions de services gérés peuvent donner lieu à l'un des trois scénarios suivants :

1. Le fournisseur de services gérés n'utilise pas de sous-processeurs en nuage
2. Le fournisseur de services gérés utilise un ou plusieurs sous-processeurs en nuage et tous les fournisseurs de services d'informatique en nuage ont déjà fait l'objet d'une évaluation de sécurité par le GC.
3. Le fournisseur de services gérés utilise un ou plusieurs sous-processeurs en nuage, et un ou plusieurs fournisseurs de services d'informatique en nuage n'ont pas fait l'objet d'une évaluation de sécurité par le GC.

Ce qu'il faut, c'est une approche pour l'acquisition de services gérés qui tient compte des trois scénarios, mais le document se concentrera sur les scénarios 2 et 3.

Le présent document vise à décrire une approche pour la prise en compte des services d'informatique en nuage avant, pendant et après le processus d'approvisionnement. Le Centre canadien pour la cybersécurité (CCC) a publié le document Contrats avec des fournisseurs de services gérés : facteurs relatifs à la cybersécurité à considérer, qui met l'accent sur les considérations en matière de sécurité des TI dans une bien plus grande mesure de ce qui est traité dans le présent document. Ce document complète le document du CCC en mettant davantage l'accent sur le processus d'approvisionnement lui-même.

Contexte

En 2016, le gouvernement du Canada a publié sa première Stratégie d'adoption de l'informatique en nuage du GC, qui précise clairement aux ministères que les services d'informatique en nuage font partie du paysage de la TI du GC et peuvent être utilisés pour héberger de l'information sensible avec une atténuation appropriée des risques. En 2018, le GC, en vertu de la Politique sur le numérique et les services, a publié une exigence « L'informatique en nuage d'abord », ce qui en fait le modèle privilégié pour déployer des services technologiques. Bien que cela n'exclue pas spécifiquement d'autres scénarios, les efforts du GC se sont concentrés, jusqu'à maintenant, sur le fait que le GC a une relation contractuelle directe avec le fournisseur de services d'informatique en nuage.

Tout comme le GC est passé à l'informatique en nuage en premier, le secteur privé l'est aussi. De plus en plus, les soumissionnaires et les fournisseurs du GC comptent sur les services d'informatique en nuage pour les aider à offrir leurs produits et services au GC.

Un fournisseur de services d'informatique en nuage est un sous-processeur de données sensibles du GC pour le fournisseur. Cela est important, car la sécurité ou les personnes, les installations et les systèmes de TI du sous-processeur doivent tous être évalués comme étant conformes à nos politiques et procédures.

Au cours de la dernière année, le GC a été témoin d'approvisionnements de services gérés et axés sur les résultats qui ont connu des retards et des interruptions importants parce que la possibilité de sous-processus en nuage n'a pas été prise en compte dans l'appel d'offres initial. Ces retards causent des frictions avec les fournisseurs et les autorités techniques.

Définitions

Aux fins du présent document, les définitions suivantes s'appliquent :

Fournisseur de services d'informatique en nuage : Des services de TI hautement commercialisés sur demande qui peuvent fournir des ressources comme le calcul et l'entreposage pour la construction d'applications d'affaires jusqu'au bout pour compléter des applications d'affaires. Les fournisseurs de services d'informatique en nuage sont les entités commerciales qui offrent ces services. Ces fournisseurs hébergent les systèmes de TI qui recueillent, stockent et traitent les données sensibles du GC.

Fournisseur de services gérés : Fournisseur du gouvernement du Canada qui offre des services opérationnels ou technologiques pour les programmes et les services du GC. Les FSG sont souvent perçus comme l'impartition d'un secteur d'activité sous la responsabilité du GC. Les FSG assument souvent la responsabilité de la prestation d'un secteur d'activité ou d'une partie de la prestation de la technologie. La relation contractuelle entre le GC et un FSG est habituellement régie par un accord sur les niveaux de service (ANS). Un FSG peut utiliser un ou plusieurs fournisseurs de services d'informatique en nuage pour fournir les composantes technologiques de ses services, comme les portails libre-service, la gestion de cas et l'analytique. Le GC n'a pas de relation contractuelle directe avec le FSIN, mais il tient plutôt le FSG contractuellement responsable des services du FSIN. Le GC est un consommateur des services du FSG et, à son tour, le FSG est un consommateur des services du FSIN.

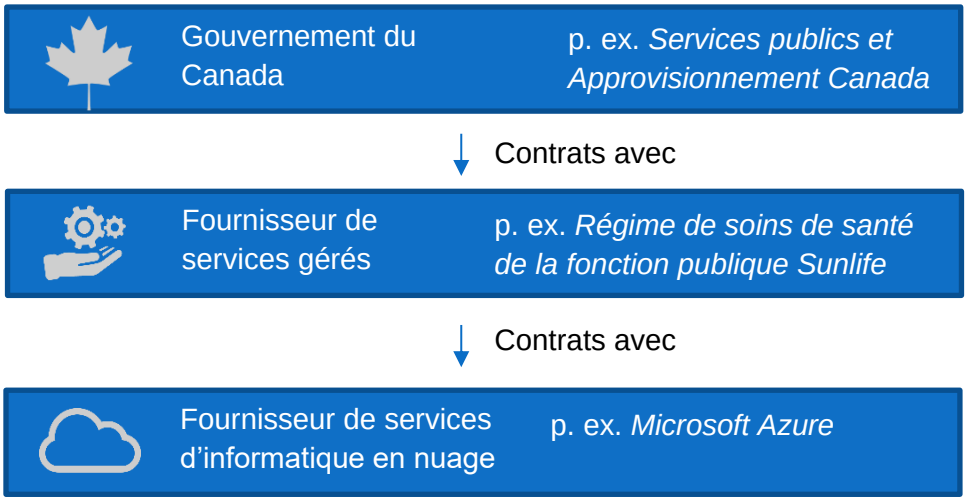


Figure 1 : Hiérarchie des relations contractuelles entre les fournisseurs

Services professionnels : Fournisseur du gouvernement du Canada qui fournit des services pour déployer, mettre en œuvre et peut-être exploiter la technologie et les services dans un environnement infonuagique. Le GC entretient une relation contractuelle avec le FSIN et le fournisseur de services professionnels. Le fournisseur de services professionnels est responsable d'accroître la capacité et les capacités du GC dans la gestion d'une composante du service du FSIN. L'obligation de rendre compte des problèmes de rendement avec le FSIN incombe toujours au GC, car le fournisseur de services professionnels n'a aucune relation contractuelle avec le FSIN.

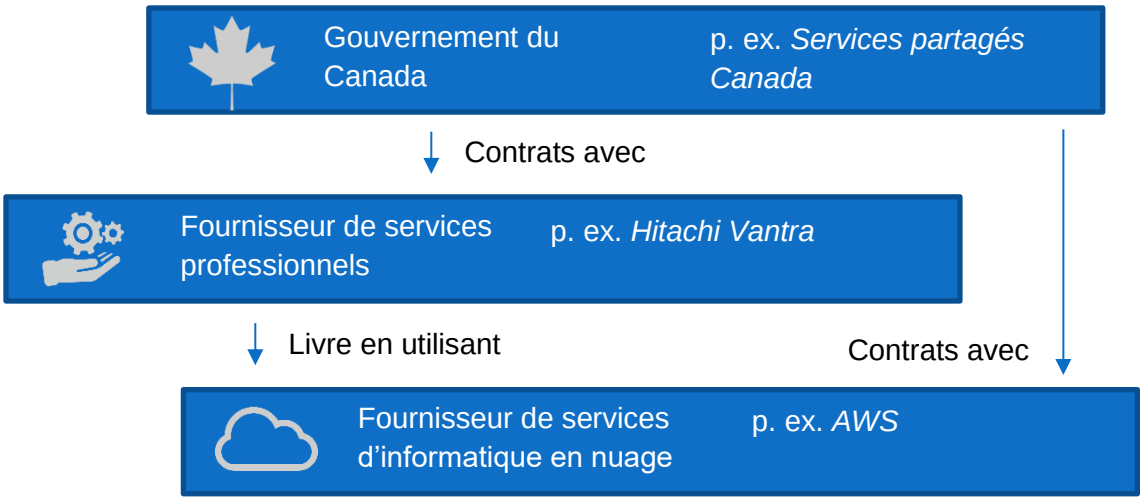


Figure 2 : Hiérarchie des relations contractuelles pour un fournisseur de services professionnels

Les fournisseurs de services professionnels ne sont pas visés par le présent document, car le GC entretient une relation contractuelle directe avec le fournisseur de services d'informatique en nuage et n'est pas un sous-processeur pour le fournisseur de services professionnels.

Approvisionnements axés sur les résultats

Dans le cadre d'un approvisionnement axé sur les résultats, il se peut que les solutions exactes à fournir ne soient pas connues au moment de l'attribution du contrat. Les soumissionnaires réagissent plutôt à un ensemble de résultats qu'ils souhaitent atteindre. Ce type d'approvisionnement peut donner lieu à des produits, à des services professionnels, à des services gérés ou à d'autres modèles de prestation. Les solutions axées sur les résultats offrent la souplesse nécessaire pour que l'ensemble de solutions puisse évoluer au fil du temps en fonction des besoins de l'utilisateur et de l'évolution de l'environnement technologique. Les fournisseurs peuvent être des fournisseurs de services d'informatique en nuage, des FSG et des IS.

Sous-traitant

SPAC affirme qu'un « sous-traitant avec lequel un fournisseur a une relation contractuelle directe pour exécuter une partie des travaux en vertu d'un contrat ou d'une entente immobilière entre le fournisseur et le Canada, à moins que le sous-traitant ne se contente de fournir des produits commerciaux standard au fournisseur »[1]

En ce qui concerne la portée des travaux exécutés dans le cadre du sous-contrat, les clauses et les exigences pertinentes s'appliquent au sous-traitant. Cela comprend les évaluations de sécurité.

Les services d'informatique en nuage sont hautement commercialisés, et le service ne change pas d'un contrat à l'autre. Au lieu de cela, la façon dont le taux préférentiel utilise le service peut être différente. Pour cette raison, les FSIN sont considérés comme des sous-processeurs, et non comme des sous-traitants. Cela ne signifie pas que le GC n'évalue pas la sécurité des fournisseurs de la sécurité de l'informatique en nuage, mais plutôt que ces évaluations sont transférables d'un contrat à l'autre.

Sous-processeur

Dans un service géré ou un approvisionnement axé sur les résultats où le fournisseur de services d'informatique en nuage n'est pas l'entrepreneur principal, il est considéré comme un sous-processeur. Le service d'informatique en nuage doit être un service commercialisé, disponible sur le marché. Il ne peut pas s'agir d'un service adapté ou créé spécifiquement pour le GC. En ce sens, un FSIN est un fournisseur de services publics, à l'instar d'une entreprise de téléphonie comme Bell Canada.

Un sous-processeur peut être évalué une fois par le GC et cette évaluation peut être utilisée pour plusieurs contrats.

Risque lié aux fournisseurs de quatrième niveau

Il s'agit du risque qui existe lorsqu'un fournisseur externalise ou utilise les services d'un autre fournisseur pour traiter ou stocker les données du client. Aux fins du présent document, le sous-processeur de nuage représente le fournisseur de quatrième niveau.

[1]https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-approvisionnements/section/4/21/3

Différenciation entre le modèle SaaS et les services gérés

Parce qu'un FSG déploie souvent des logiciels dans un environnement d'infrastructure en nuage et les offre à un consommateur, un FSG et un SaaS peuvent être facilement confondus. La principale différence entre un SaaS et un FSG repose dans le fait que dans un SaaS, le service est hautement commercialisé. Dans un SaaS, de nombreux consommateurs sont locataires au sein du même service. Imaginez un immeuble où chaque consommateur a un appartement. Chaque consommateur loue une partie de l'immeuble. Cela ressemble au SaaS. Aucun investissement n'était requis par les locataires pour que l'immeuble soit construit. Ils commencent tout simplement à louer l'appartement et, à la fin de leur bail, ils cessent de payer le loyer. Dans un service géré, bien qu'un sous-processeur SaaS puisse être impliqué, le FSG personnalise l'offre ou la combine avec d'autres pour créer une nouvelle offre. Habituellement, cette offre s'adresse à un seul consommateur, le GC.

Il faut aussi savoir que certains fournisseurs qualifient leur service géré de SaaS, de SaaS géré ou de SaaS privé. La nomenclature et le marketing à eux seuls ne suffisent pas à déterminer si l'offre de service est un SaaS ou un service géré. Le tableau ci-dessous distingue plutôt certaines des caractéristiques de chaque modèle.

La différence entre un service géré et un SaaS entraîne des approches différentes en matière de sécurité, d'approvisionnement et des profils de risque différents.

Services gérés	**Logiciel comme service**
Sur mesure	Commercialisé
Conçu ou hautement personnalisé pour un consommateur	Service préexistant, disponible sur le marché
Les accords sur les niveaux de service peuvent être adaptés au consommateur	Les ententes sur les niveaux de service sont préétablies et sont souvent accessibles au public pour tous les consommateurs.
Les prix sont adaptés au consommateur	Les prix sont disponibles sur le marché, des rabais sur le volume sont offerts.
Les nouvelles fonctions entraînent généralement des demandes de modification de contrat.	L'innovation et les nouvelles caractéristiques n'exigent aucun investissement de la part des consommateurs
Les caractéristiques sont déterminées par le titulaire du contrat	Feuille de route des caractéristiques et des produits déterminée par les données des consommateurs et du marché
Les consommateurs peuvent demander que les changements, les mises à jour et les fonctionnalités soient mis en attente.	Le consommateur doit évoluer au rythme de l'innovation
Nécessite une approche d'évaluation de la sécurité adaptée	Détient habituellement des certifications de sécurité reconnues à l'échelle internationale, comme ISO et SOC
L'intégration peut prendre des semaines ou des mois pendant que le fournisseur adapte ou construit le service.	L'intégration devrait prendre quelques minutes. Le service est préexistant.

Évaluation des qualifications en matière de sécurité du service géré

Lorsqu'un service géré comprend un fournisseur d'informatique en nuage comme sous-processeur, une évaluation de sécurité du FSG et du FSIN est requise, mais l'approche est différente pour les deux. De plus, il peut y avoir des scénarios où un sous-processeur compte sur un autre sous-processeur (reportez-vous à la figure 3).

Cette section ne se veut pas un aperçu complet de l'évaluation de la sécurité d'un FSG. Le CCC a publié le document Contrats avec des fournisseurs de services gérés : facteurs relatifs à la cybersécurité à considérer, qui fournit des directives plus complètes en matière de sécurité. Cette section vise plutôt à aider le lecteur à comprendre les différentes approches du FSG par rapport à celles des sous-processeurs en nuage.

Dans le cas d'un FSG, les systèmes de TI utilisés par le fournisseur doivent faire l'objet d'une évaluation de sécurité conformément à la gestion des risques liés à la sécurité des TI :Une méthode axée sur le cycle de vie (ITSG-33) Si le FSG utilise un ou plusieurs FSIN comme sous-processeurs, le FSG utilisera les évaluations de sécurité de tous les FSIN comme preuve à l'appui de la partie du système de TI exploité par le ou les FSIN. Lors de la collecte des données d'évaluation pour le ou les FSIN, l'un des deux scénarios suivants peut se présenter :

1. Le GC dispose d'une évaluation à jour du FSIN. Dans ce scénario, le GC a évalué la sécurité du FSIN et aucune autre évaluation n'est requise. La liste complète des fournisseurs qui ont été évalués par le GC se trouve à https://cloud-broker.canada.ca/s/?language=fr

2. Le GC n'a pas encore évalué le FSIN. Dans le cadre de ce scénario, une évaluation devra être effectuée conformément au modèle d'assurance des niveaux d'informatique en nuage du GC.

L'évaluation des qualifications en matière de sécurité du fournisseur peut avoir lieu au cours d'une ou de plusieurs des phases d'approvisionnement suivantes :

- *Évaluation des soumissions*. L'évaluation des qualifications de sécurité du FSG créera un processus d'évaluation plus long, mais le GC aura la certitude des qualifications de l'entrepreneur avant l'attribution du contrat. Une partie ou la totalité des activités d'évaluation de la sécurité peuvent avoir lieu pendant l'évaluation des soumissions.

- *Exécution, avant lelancement*. Après l'attribution du contrat, mais avant le lancement du service, des activités d'évaluation peuvent avoir lieu. Cela est particulièrement utile pour les approvisionnements axés sur les résultats lorsque la nature exacte de la solution n'est pas connue pendant l'évaluation des soumissions. De plus, les soumissionnaires pourraient ne pas vouloir investir dans des activités d'évaluation détaillées avant l'attribution du contrat.

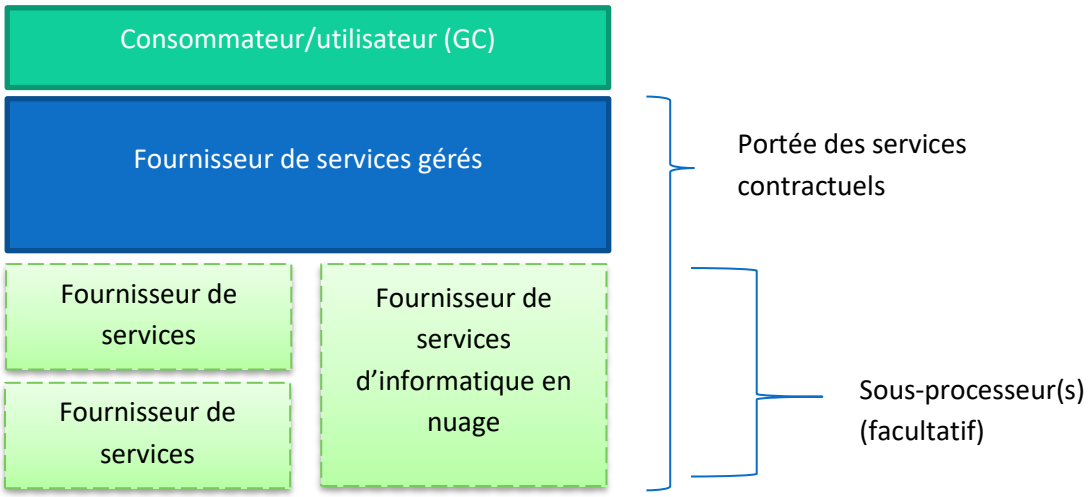


Figure 3 : Hiérarchie des relations héritées en matière de sécurité et de passation de marchés

Évaluation des qualifications en matière de sécurité des fournisseurs de services d'informatique en nuage

Cette section n'est pas une vue d'ensemble de l'évaluation de la sécurité des fournisseurs de services d'informatique en nuage. Des procédures plus complètes sont disponibles dans le document intitulé Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage du gouvernement du Canada. Cette section vise plutôt à fournir au lecteur un aperçu de ce que les fournisseurs de services en nuage doivent évaluer. Les fournisseurs de services d'informatique en nuage, que ce soit directement à forfait ou en tant que sous-processeurs de services gérés ou de fournisseurs axés sur les résultats, doivent subir des évaluations de sécurité liées à la catégorisation des données qu'ils traitent. L'un des principaux objectifs de l'évaluation par le GC des qualifications en matière de sécurité du fournisseur de services d'informatique en nuage est d'évaluer le fournisseur une fois en fonction du modèle d'assurance des niveaux d'informatique en nuage du GC et non pour chaque contrat pour lequel il est un fournisseur ou un sous-processeur. Cela s'explique par le fait que l'offre de services d'un fournisseur de services d'informatique en nuage est hautement commercialisée et ne change pas avec chaque processus d'approvisionnement. Il s'agit d'une différence clé par rapport aux modèles de TI traditionnels où l'offre change souvent en fonction des exigences de chaque processus d'approvisionnement. Un fournisseur d'informatique en nuage n'a besoin d'être évalué qu'une seule fois (et de rester conforme), mais d'appliquer cette évaluation à de multiples contrats.

Un autre élément clé de l'évaluation des fournisseurs de services d'informatique en nuage est l'utilisation de certifications de sécurité reconnues à l'échelle internationale comme ISO270017 et SOC 2 comme preuve de la conformité aux contrôles de sécurité des TI du GC.

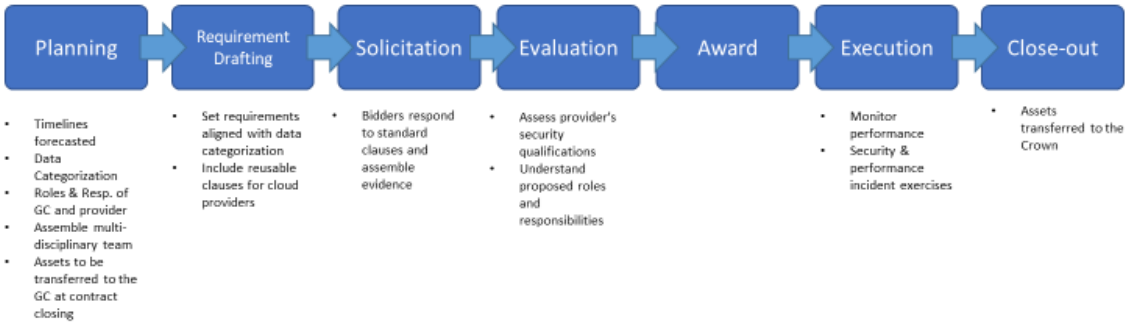
L'évaluation d'un fournisseur de services d'informatique en nuage exige que l'organisation, le personnel, les installations, les contrôles de sécurité des TI, les politiques et les procédures soient tous évalués.

Les ministères, dans le cadre d'un processus d'approvisionnement, doivent exiger que les fournisseurs de services d'informatique en nuage subissent les évaluations de sécurité suivantes :

	Qui évalue	**Comment les exigences sont-elles déterminées?**	**Quand l'évaluation est-elle effectuée?**
Enquête de sécurité sur l'organisation	Programme de sécurité des contrats de SPAC	Veuillez remplir la LVERS avec le Guide de classification (exemple fourni à l'annexe B)	Avant l'attribution du contrat
Vérification des installations Les installations qui stockent des données protégées doivent faire l'objet d'une vérification.	Programme de sécurité des contrats de SPAC	Veuillez remplir la LVERS avec le Guide de classification (exemple fourni à l'annexe B)	Avant l'attribution du contrat
Personnel Le personnel qui accède aux données protégées doit faire l'objet d'une vérification.	Programme de sécurité des contrats de SPAC	Veuillez remplir la LVERS avec le Guide de classification (exemple fourni à l'annexe B)	Avant l'attribution du contrat
Programme d'évaluation de l'informatique en nuage	Reportez-vous au modèle d'assurance des niveaux d'informatique en nuage du GC.	Reportez-vous aux clauses modèles à l'annexe A.	Une fois que le ou les soumissionnaires retenus sont déterminés

Approche pour la comptabilisation de l'informatique en nuage dans les approvisionnements

L'approche pour la comptabilité ou les sous-processeurs en nuage est intégrée tout au long du cycle de vie de l'approvisionnement.



Planification

La planification précoce peut aider à gérer les attentes en matière d'activités de conformité et d'évaluation tout en réduisant la friction avec tous les intervenants. La planification du dernier jour du contrat peut également aider à établir des exigences pour éviter le blocage et le transfert d'actifs, comme des données, afin de faciliter le lendemain de la fin du contrat. Les activités particulières devraient comprendre :

- **Catégorisez vos données.** La connaissance de la catégorisation de vos données orientera de nombreuses décisions en aval concernant les exigences et la portée des intervenants participant au processus d'approvisionnement. L'approvisionnement axé sur les résultats peut servir une vaste gamme de solutions. Si la catégorisation exacte des données n'est pas connue au départ, d'autres approches peuvent être adoptées. Par exemple, vous pourriez vouloir établir un « point culminant » représentant la plus haute catégorisation de données possible pour le ou les contrats subséquents. Toutefois, cela pourrait exclure les soumissionnaires et les solutions pour ce qui peut être une petite portée de données très sensibles. La création de niveaux où les soumissionnaires peuvent répondre à un niveau croissant d'exigences associées à une sensibilité accrue est une autre approche. Cela offre une grande souplesse, mais ajoutera probablement de la complexité au processus d'évaluation.
- **Faites référence au modèle des niveaux d'informatique en nuage du GC** (lien requis). La catégorisation des données, combinée à la portée des utilisateurs de la solution, détermineront les intervenants en matière de sécurité qui pourraient devoir participer au processus

d'approvisionnement. Pour les solutions d'entreprise (à l'échelle du GC), le CCC sera probablement un intervenant et sa participation devra être planifiée.

- **Déterminez les rôles et les responsabilités :** Il est essentiel de comprendre les rôles et responsabilités des fournisseurs par rapport à ceux du GC pour satisfaire aux exigences en matière de sécurité et de rendement. Dans le cadre d'une prestation gérée, le fournisseur sera tenu responsable de la performance et de la sécurité des activités relevant de son champ de responsabilité. Dans le cas des approvisionnements axés sur les résultats, les rôles et responsabilités exacts du fournisseur pourraient ne pas être connus. Dans ce cas, ces rôles et responsabilités devraient être énoncés clairement lorsqu'il y a une commande subséquente ou une autorisation de tâches pour des services en vertu du contrat.
- **Établir un horaire et constituer une équipe.** Avec la participation des principaux intervenants, établir un horaire. L'accent devrait être mis sur la participation de l'équipe aux étapes de la rédaction des exigences et de l'évaluation de l'approvisionnement. Pendant la rédaction, les évaluateurs de la sécurité devront avoir une stratégie pour évaluer les qualifications en matière de sécurité des soumissionnaires. Cela comprendra la participation de SPAC, de DSIC, du CCC, des évaluateurs de la sécurité des TI de votre ministère. Leurs activités d'évaluation détermineront les exigences de la DP. Au cours des phases d'évaluation, ces mêmes membres de l'équipe exécuteront leurs activités d'évaluation. Les autorités techniques du responsable opérationnel devront énoncer les résultats, les attentes en matière d'accord sur les niveaux de service et les responsabilités du ou des fournisseurs.
- **Planifiez le dernier jour du contrat.** Dans les services gérés et les ententes axées sur les résultats, le fournisseur héberge souvent des données sensibles au nom du GC. Au début, le GC doit comprendre ces biens et expliquer comment ils seront transférés au GC ou transférés à un nouveau fournisseur à la fin de la période du contrat. De plus, il faut indiquer clairement si le fournisseur peut conserver ces données ou s'il doit les détruire.

Rédaction des exigences

- **Inclure des clauses tenant compte du nuage.** Au début, vous n'avez peut-être aucune idée si le ou les soumissionnaires retenus incluent des sous-processeurs en nuage dans les services ou les solutions. Pour cette raison, un ensemble de clauses modèles a été créé pour tenir compte de cette possibilité. Ces clauses se trouvent à l'annexe X.
- **Exigences relatives à la définition des rôles et des responsabilités**. Habituellement, les exigences en matière de services gérés définissent le rôle du fournisseur par rapport à celui du GC, mais ce n'est pas toujours le cas. Souvent, le GC demande aux soumissionnaires de faire preuve de souplesse pour suggérer la portée des services qu'ils peuvent offrir. Dans ce cas, dans le cadre de la réponse du soumissionnaire, ils devraient être tenus de décrire les responsabilités du fournisseur, de ses sous-processeurs, par rapport à celles du GC sous la forme d'une matrice de responsabilité, de responsabilisation, de consultation et d'information (RACI). Dans le cas des approvisionnements axés sur les résultats, cela pourrait ne pas être connu au moment de l'attribution du contrat, auquel cas le fournisseur devrait être tenu de décrire l'approche RACI au moment de l'autorisation de tâches.

Demande de soumissions

À cette étape, les soumissionnaires potentiels répondent aux exigences du GC et posent des questions de clarification.

Évaluation

La phase d'évaluation des soumissions permet à l'équipe d'évaluation d'examiner en premier lieu les modèles, les services et les qualifications en matière de sécurité des services proposés par le fournisseur. Le niveau de détail fourni dans les soumissions dépendra des exigences de l'exigence originale. Il y a des raisons valables d'être plus précis dans vos exigences pendant la phase de demande de soumissions et des raisons valables d'attendre à la phase d'exécution pour obtenir ces détails. Le fait de demander plus de détails à l'étape de la demande de soumissions fera augmenter les coûts de chaque soumissionnaire et créera une étape d'évaluation plus complexe. Dans les approvisionnements axés sur les résultats, la nature exacte des solutions proposées n'est probablement pas encore connue avant la phase d'exécution.

Si possible, la phase d'évaluation devrait déterminer :

- Les rôles et responsabilités du fournisseur, du FSG et de tout sous-processeur. Connaître les rôles et les responsabilités de chacun par rapport à ceux du GC aidera à comprendre la portée de l'évaluation de sécurité requise pour chacun.
- Dans la mesure où les clauses modèles ont été utilisées, les soumissionnaires doivent indiquer, dans leur soumission, s'ils font appel à des fournisseurs de services d'informatique en nuage qui sont des sous-processeurs. Cela mènera à l'une des trois possibilités suivantes :
    1. Aucun sous-processeurs en nuage. Dans ce scénario, le FSG exploite tous les systèmes de TI et les procédures d'évaluation de la sécurité décrites dans la Gestion des risques liés à la sécurité des TI :Une méthode axée sur le cycle de vie (ITSG-33) peut être utilisée.
    2. Tous les fournisseurs d'informatique en nuage ont été évalués par le GC. Dans ce scénario, aucune autre activité d'évaluation axée sur les sous-processeurs n'est nécessaire. Toutes les activités d'évaluation de la sécurité peuvent être axées sur le FSG.
    3. Le GC n'a pas évalué un ou plusieurs sous-processeurs en nuage. Dans ce cas, les FSIN sans évaluation préalable et le FSG doivent être évalués. Pour le FSIN, le modèle d'assurance des niveaux d'informatique en nuage du GC déterminera qui effectue les activités et quelles sont ces dernières en fonction de la catégorisation des données et de la portée des utilisateurs.

Attribution

Aux fins du présent document, aucune activité n'a été incluse.

Exécution

Une fois le contrat attribué, l'intégration du fournisseur peut commencer. Cette phase est divisée en deux sous-phases. Les activités sont divisées en activités avant et après le lancement.

Avant le lancement

Avant le lancement du service, les activités suivantes sont requises :

- Toutes les évaluations de sécurité qui n'ont pas été effectuées pendant l'évaluation du contrat doivent l'être avant le lancement du service.

- Veuillez établir un processus d'intervention en cas d'incident de sécurité. Étant donné que de multiples intervenants peuvent participer à l'intervention en cas d'incident, il est essentiel d'avoir un plan d'intervention.

Après lancement

Après le lancement du service, les activités suivantes doivent avoir lieu :

- Changement de sous-processeurs. Si le fournisseur change de sous-processeurs, ces sous-processeurs devront être évalués avant la mise en œuvre des changements. De plus, si le GC
- Conformité continue. Veillez à ce que les sous-processeurs existants des fournisseurs demeurent en règle au fil du temps.
- Effectuez des exercices d'intervention en cas d'incident de sécurité. À l'aide du plan d'intervention en cas d'incident établi précédemment et des scénarios d'incident, effectuez des simulations ou des exercices pour vous assurer que tout le monde comprend ses rôles et responsabilités.

Clôture

À la clôture du contrat, assurez le transfert des ressources d'information au GC ou au nouveau fournisseur. Au besoin, assurez-vous que le fournisseur dispose des données du GC.

Modification des modèles de service après le lancement

Jusqu'à maintenant, le document a mis l'accent sur la progression linéaire des activités, mais qu'arrivera-t-il si le fournisseur de services gérés change les modèles de prestation après l'attribution du contrat? Si l'approche décrite dans le présent document est suivie, les exigences devraient permettre l'utilisation de modèles de TI traditionnels et de modèles en nuage. Si le fournisseur souhaite modifier le modèle de prestation ou changer de fournisseur, il devra se conformer aux exigences en matière de sécurité, de protection des renseignements personnels et d'évaluation liées aux services d'informatique en nuage dans la demande de soumissions initiale.

Sommaire de l’orientation

Cette section se veut un aperçu de haut niveau de l’orientation fournie dans le présent document.

1. Tous les approvisionnements de services gérés et axés sur les résultats devraient tenir compte des fournisseurs d’informatique en nuage en tant que sous-processeurs.
2. Catégorisez les données qui seront traitées par le fournisseur, car elles entraîneront des décisions critiques. Même lorsque le périmètre exact des données n’est pas connu au départ, il est conseillé de choisir une limite supérieure aux données qui seront traitées par le(s) fournisseur(s).
3. En vertu des rôles et responsabilités du fournisseur de services géré, des sous-processeurs de l’informatique en nuage et du GC dans la prestation et la gestion du service. Cela aidera à déterminer la portée de l’évaluation de la sécurité pour chaque rôle.
4. Le modèle d’assurance des niveaux d’informatique en nuage du GC aidera à déterminer les intervenants qui doivent être inclus dans les évaluations de sécurité et orientera le calendrier du chemin critique.
5. Utilisez les clauses et exigences du modèle à l’annexe A pour tenir compte des fournisseurs de services en nuage en tant que sous-processeurs
6. Bien que le document ne porte pas sur les scénarios de services professionnels, lorsque ce scénario se produit, il est préférable d’utiliser les contrats existants à l’échelle de l’entreprise pour fournir les services d’informatique en nuage que le fournisseur de services professionnels utilisera.

Appendix A – Template Clauses

Note: clauses taken from PSHCP RFP found here:
https://buyandsell.gc.ca/cds/public/2020/08/31/2392d112167c01e82a59483e1e0cb68b/ABES.PROD.PW__XF.B002.E38428.EBSU000.PDF

Pre-launch

Purpose: Requires that, when an MSP uses a cloud sub-processor, the MSP provides the certification assessment reports of the CSP to the GC prior to the service launching.

When should the requirement be met?: pre-launch of service (Service Ready Date)

Protected B, Medium Integrity and Medium Availability for cloud sub-processors (If Applicable)

i. If the Contractor's solution includes one or more cloud-based solution, The Contractor must obtain Project Authority Approval, prior to the Service Ready Date, that the Contractor is in compliance with the security requirements selected in the Government of Canada Cloud Security Risk Management Approach and Procedures.

https://www.canada.ca/en/government/system/digital-government/digitalgovernment-innovations/cloud-services/cloud-security-risk-managementapproach-procedures.html

ii. The Contractor must provide certification or assessment reports. The Contractor must meet the Government of Canada public cloud security requirements for information and services up to Protected B

Threat Monitoring

Purpose: Requires that log information be provided to the GC for threat monitoring purposes. The depth of logs to be provided depends upon the cloud service model being used.

When should the requirement be met?: pre-launch of service (Service Ready Date)

a) For cloud-based environments:

i. The Contractor must allow for application data and associated network traffic to be copied and forwarded to a Government of Canada approved location.

ii. The Contractor must deploy and operate security software to perform advanced monitoring and mitigations of cyber threats for the services at the Contractor's managed host and network layer, for all components managed by the Contractor.

iii. All events and logs for systems supporting the service must be forwarded to a Government of Canada approved system. Alternatively, the Contractor must provide APIs that provide the ability to:

a) Inspect and interrogate data at rest in SaaS applications; and

b) Assess events such as user access and behaviour, administrator access and behaviour, and changes to third-party API access, stored in SaaS application logs.

Continuity Management

Purpose: Ensures that if the MSP must meet priority of service requirements that their cloud sub-processors must also comply with those requirements.

When should the requirement be met?: pre-launch of service (Service Ready Date)

In the event that the Contractor subcontracts or leverages a cloud solution, they must ensure that all dependencies on subcontractor and/or cloud solutions must provide a similar priority of service.

Third-Party Assurance and Certifications

Purpose: Ensures that if the MSP uses cloud service providers as sub-processors, those CSP must maintain valid security certifications through-out the life of the contract.

When should the requirement be met?: Through-out execution until close-out

The Contractor must maintain the following valid and up-to-date industry certifications for the period of the Contract:

a) ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems – Requirements; (see https://www.iso.org/standard/54534.html)

b) ISO/IEC 27017:2015 Information technology (see https://www.iso.org/standard/43757.html) -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 (see https://www.iso27001security.com/html/27002.html) for cloud services; and

c) AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, privacy and confidentiality - issued by an independent Certified Public Accountant.

ii. Each certification or audit report provided must:

(i) identify the legal business name of the Contractor or applicable Sub-processor;
(ii) identify the Contractor's or Sub-processor's certification date and the status of that certification;
(iii) identify the services included within the scope of the certification report. If the carved-out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor. iv. Each SOC 2 Type II audit report must have been performed within the 12 months prior to the Operations Ready Date. A bridge letter may be provided to demonstrate that the Contractor is in process of renewal where there is a gap between the service organization's report date and the user organization's year-end (i.e., calendar or fiscal year-end). v. The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, and SOC 2 Type II for the period of the Contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

Cloud Service Provider (CSP) IT Security Assessment Program

Purpose: If the MSP changes IT deployment model to cloud, the MSP must provide perform the appropriate secure assessment activities and provide the appropriate evidence.

When should the requirement be met?: Through-out execution until close-out

i. If during the period of the Contract and following the approval of the Project Authority, the Contractor migrates the application and/or data from an on premise to a Cloud-based solution, the Contractor must demonstrate that the Cloud Service Provider:

a) Is compliant with the security requirements selected in the Government of Canada Security Control Profile for Cloud-Based Services for GC Services (https://www.canada.ca/en/government/system/digital-government/digitalgovernment-innovations/cloud-services/government-canada-security-controlprofile-cloud-based-it-services.html) for Cloud Services that are leveraged for the solution; and

b) Has been assessed under the Canadian Centre for Cyber Security (CCCS) CSP Information Technology (IT) Security Assessment Process(ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technologysecurity-assessment-process-itsm50100

ii. Any Cloud Service Provider that has participated in the process must provide documentation to confirm that they have completed the onboarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS.

iii. To initiate the on-boarding process, the Cloud Service Provider should contact the CCCS Client Services to receive a copy of the onboarding submission form and any additional information related to the CSP IT Assessment Program.

Appendix B – Sample SRCL and Classification Guide

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
32099-11
Security Classification / Classification de sécurité
UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

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

2. Branch or Directorate / Direction générale ou Direction
Procurement and Vendor Relations

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

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

4. Brief Description of Work / Brève description du travail
To procure commercially available software up to the level of Protected B

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

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

6. Indicate the type of access required / Indiquer le type d'accès requis

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

6. b) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets is/are released within a foreign country? / Le fournisseur et ses employés (par exemple : gardes, entretien et nettoyage, etc.) auront-ils accès à des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS qui sont divulgués à l'étranger? (Specify the level of access using the chart in Question 7. c) / Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) — No / Non ☑ — Yes / Oui ☐

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

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

Canada ☑ — NATO / OTAN ☐ — Foreign / Étrangère ☐

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

No release restrictions / Aucune restriction relative à la diffusion ☑

All NATO countries / Tous les pays de l'OTAN ☐

No release restrictions / Aucune restriction relative à la diffusion ☐

Not releasable / Ne pas diffuser ☐

Restricted to / Limitée à : ☐ — Specify country(ies) / Préciser le(s) pays :

Restricted to / Limitée à : ☐ — Specify country(ies) / Préciser le(s) pays :

Restricted to / Limitée à : ☐ — Specify country(ies) / Préciser le(s) pays :

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

PROTECTED A / PROTÉGÉ A	☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	☐	PROTECTED A / PROTÉGÉ A	☐
PROTECTED B / PROTÉGÉ B	☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	☐	PROTECTED B / PROTÉGÉ B	☐
PROTECTED C / PROTÉGÉ C	☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐	PROTECTED C / PROTÉGÉ C	☐
CONFIDENTIAL / CONFIDENTIEL	☐	NATO SECRET / NATO SECRET	☐	CONFIDENTIAL / CONFIDENTIEL	☐
SECRET / SECRET	☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET	☐	SECRET / SECRET	☐
TOP SECRET / TRÈS SECRET	☐			TOP SECRET / TRÈS SECRET	☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	☐			TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	☐

TBS/SCT 350-103 (2004/12)

Security Classification / Classification de sécurité
UNCLASSIFIED

Canada

Appendix A – Security Classification Guide

The following table outlines the personnel and facility security clearance requirements based on the expected roles and access to GC data.

Table A-1 Security Classification Guide for Commercial Cloud Services

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required[1]	Responsibility	Details
1.	Any Contractor personnel with physical access to the Contractor data centers	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local Backup Media	Canada	Reliability	Contractor	This is for any Contractor personnel including facilities management resources that have physical access to the Cloud Services hardware equipment at the Contractor data centers.
2.	Any Contractor personnel who have logical access to the Contractor services	• All Business Data • Data as stored on the Contractor's compute, storage, and network components	Both	Reliability	Contractor	This is for any Contractor personnel that has logical access to the GC data hosted in the Contractor data centers and any sensitive system and security incident data.
3.	Any Contractor personnel with privileged roles and unrestricted logical access to GC assets within the Contractor services	• All Business Data • GC Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components • Assets include GC data and credentials	Both	Secret	Contractor	This is for any Contractor personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the Contractor data centers and any sensitive system and security incident data.
4.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[1] Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada.

Document history

V0.02 – Nov 2020	Initial drafting based upon working group discussions
V0.03 – Dec 2020	Feedback from OCIO Cyber – added fourth party vendor risk Added explanation of SaaS and managed services
V0.04 – Dec 2020	Feedback from CCCS including • Clarifications on language and explanation • Highlight the need for GC to have NDA with CSP to get ISO and SOC reports • Changed definition of a system integrator to professional services provider • GC Cloud Tiered Assurance Model clarifications • Use of CCCS published controls in lieu of TBS controls