ÉBAUCHE POUR CONSULTATION

Processus de présélection des solutions de services de sécurité basés sur l'infonuagique (SSBI)

But:

Le but de ce processus de présélection est de qualifier et de classer les solutions de Services de sécurité basés sur l'infonuagique (SSBI) en fonction d'un ensemble de critères obligatoires et cotés qui permettront au Canada de classer les solutions les mieux notées, y compris une solution réservée dont le fournisseur d'équipement original (FEO) est une petite et moyenne entreprise (PME). Les FEOs des solutions les mieux notées seront invités à signer un contrat pour effectuer la preuve de concept afin que le Canada puisse travailler avec le FEO afin que la solution proposé rencontre les exigences viables minimales obligatoires (EVM) et pour comparer les solution entre elles afin de sélectionner les meilleures solutions pour le Canada. Le résultat de ce processus est un ensemble de solutions qualifiées.

Une fois les solutions qualifiées, le Canada procédera à la qualification de FEO et de revendeurs pour chaque solution qualifiée et attribuera une offre à commandes à ceux qui se qualifieront. Par la suite, le Canada sélectionnera le fournisseur de la solution sélectionné pour le déploiement d'entreprise de SPC.

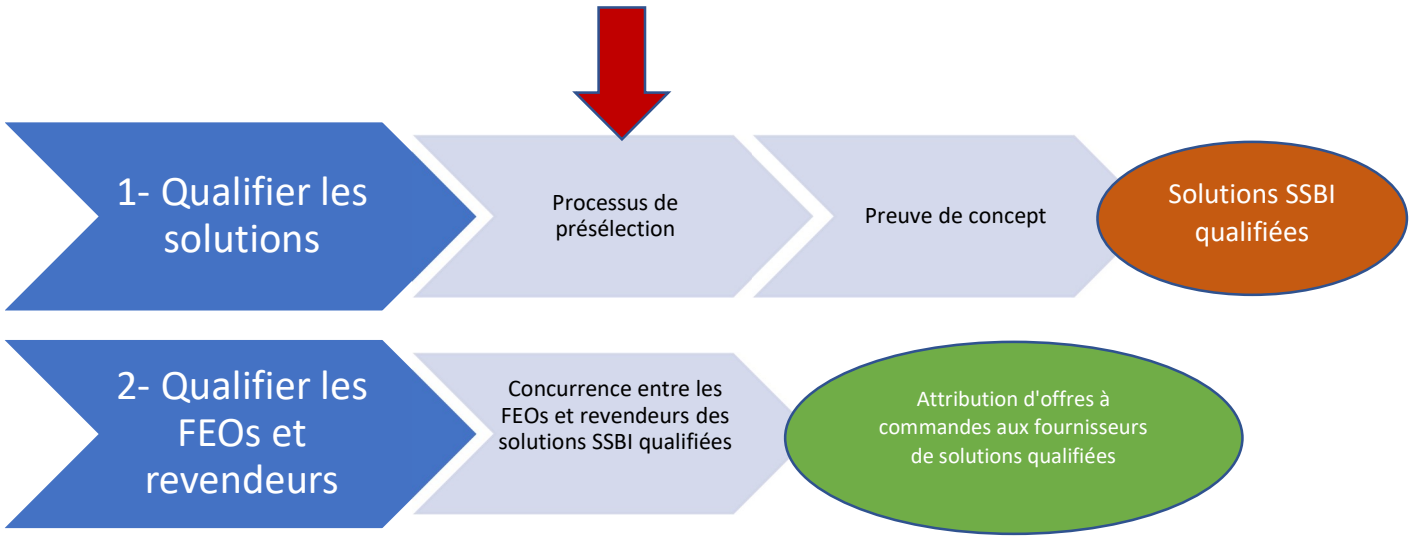

Figure 1 : Diagramme du processus proposé

Processus :

La présélection applique des critères fondés sur des preuves qui seront évalués et notés à l'aide d'un processus en 3 parties comme suit :

- Partie A – Certification et exigences obligatoires : Les FEOs de la solution doivent répondre par écrit à un ensemble de certifications requises et à un premier ensemble de critères obligatoires et évalués.
    - Pour être jugée recevable, la soumission de la solution OEM doit être conforme aux certifications et satisfaire aux exigences obligatoires.
    - Les FEOs de solutions non recevables recevront des commentaires et une opportunité de corriger leur réponse pour toutes certifications non satisfaites ou pout les exigences obligatoires.
    - Les FEOs de solutions recevables seront invités à passer à la partie B.

- Partie B - Réponse écrite cotée par points et session virtuelle interactive : la réponse écrite aux critères cotés sera évaluée par l'équipe d'évaluation. Les FEOs de la solution seront invités à une session virtuelle interactive de 75 minutes pour démontrer leur capacité à répondre à un deuxième ensemble de critères cotés par points.

Le Canada peut décider d'inviter les huit (8) solutions des FEO les mieux classés à une étape de démonstration.

Le Canada peut décider de passer directement à la preuve de concept dans les cas suivant :

- si 6 solutions ou moins sont recevables ; ou
- si 6 solutions ou moins ont obtenu un score total de 32 points ou plus à la partie B *Réponse écrite cotée et session virtuelle interactive*. Un total de 43 points cotés sont disponibles.

Les quatre (4) premières solutions de FEO classées seront invitées à soumettre une proposition financière pour la preuve de concept conformément au CPDOC et à l'énoncé des travaux. Les autres solutions recevables de FEOs, le cas échéant, resteront en attente.

Si, au cours de la preuve de concept, un ou plusieurs solutions recevables de FEOs ne satisfont pas aux exigences minimales viables, le Canada peut inviter la solutions FEO recevables suivante dans la file d'attente à participer.

Partie A – Certifications et critères obligatoires

Certifications

Les certifications suivantes doivent être soumises dans le cadre de la partie A du processus de présélection en remplissant le tableau ci-dessous avec la signature, le nom et le titre d'une personne autorisée à signer au nom du FEO de la solution.

Tableau 1 : Certifications

Certifications	**Auto-évaluation**		**Signature** **Nom et titre de la person authorisé à signé pour le FEO de la solution proposée**
	Satisfait	**Non satisfait**	
C1 : Certification du fabricant d'équipement d'origine (FEO) **Je certifie que je suis le FEO de la solution SSBI proposée.** La définition de FEO est la suivante : l'entreprise qui fabrique les produits (le fabricant "d'origine").			
C2 : Certification de la solution SaaS **Je certifie que la solution CBSS proposée est une solution Software as a Service (SaaS).** *La définition du SaaS est la suivante :* *Logiciel détenu, livré et géré à distance par un ou plusieurs fournisseurs. Le fournisseur fournit un service logiciel basé sur un ensemble de définitions de code et de données communes qui est consommé dans un modèle un-à-plusieurs par tous les clients sous contrat à tout moment sur une base de paiement à l'utilisation ou sous forme d'abonnement basé sur des mesures d'utilisation.*			
C3 : Certification de conformité des cas d'utilisation SSBI Je certifie que la solution CBSS proposée peut répondre aux cas d'utilisation définis dans le document SPDOC, pièce jointe A - Énoncé du défi. Les titres de chaque cas d'utilisation sont fournis ci-dessous pour plus de facilité : • Cas d'utilisation 1a : Utilisateur mobile (appareil géré) accédant à des services basés sur le cloud • Cas d'utilisation 1b : Utilisateur mobile (appareil géré) accédant aux services GC sur site (EDC) • Cas d'utilisation 2a : Utilisateur mobile (appareil non géré par GC) accédant aux services infonuagiques • Cas d'utilisation 2b : Utilisateur mobile (appareil non géré par le GC) accédant aux services sur place (EDC) du GC • Cas d'utilisation 3a : Utilisateur BYOD accédant à des services basés sur le cloud • Cas d'utilisation 3b : Utilisateur BYOD accédant aux services GC sur site (EDC) • Cas d'utilisation 4a : accès des utilisateurs à l'Internet des objets (IoT)/aux appareils scientifiques via Internet • Cas d'utilisation 4b : les appareils IoT/scientifiques accèdent à d'autres appareils ou systèmes IoT/scientifiques via Internet • Cas d'utilisation 5a : Utilisateur externe utilisant un appareil non géré par le GC ou BYOD accédant aux services infonuagiques du GC			

Certifications	Auto-évaluation		Signature Nom et titre de la person authorisé à signé pour le FEO de la solution proposée
	Satisfait	Non satisfait	
• Cas d'utilisation 5b : Utilisateur externe utilisant un appareil non géré par GC ou BYOD accédant aux services GC sur site (EDC) • Cas d'utilisation 6a : Utilisateur (appareil géré) sur un site distant du GC accédant aux services infonuagiques • Cas d'utilisation 6b : Utilisateur (appareil géré) sur un site distant du GC accédant aux services du GC sur site (EDC) • Cas d'utilisation 7 : Utilisateur avec un appareil géré sur un site distant du GC accédant aux services infonuagiques via Internet et aux services du GC sur site (EDC) via un hub régional			
C4 : Certification de gestion multi-locataires Je certifie que la solution SSBI proposée fournit une gestion multi-locataires pour permettre aux administrateurs du GC de différentes organisations de gérer, de générer des rapports personnalisés et d'administrer des parties spécifiques de la solution dans leur domaine autorisé, comme suit : • L'administrateur 1 peut gérer, administrer et générer des modèles de rapports personnalisés pour le locataire 1. • L'administrateur 1 ne peut pas gérer, administrer ou générer des rapports modèles et personnalisés pour le locataire 2. • L'administrateur 2 peut gérer, administrer et générer des modèles de rapports personnalisés pour le locataire 2. • L'administrateur 2 ne peut pas gérer, administrer ou générer des modèles de rapports personnalisés pour le locataire 1. • L'administrateur 3 peut gérer, administrer et générer des modèles de rapports personnalisés pour les locataires 1, 2 et le service dans son ensemble. Définitions liées à la gestion multi-locataires : Dans le contexte du processus de présélection du SSBI, plusieurs domaines, ou multi-locataire désignent un mode de fonctionnement d'un logiciel où plusieurs instances indépendantes d'une ou plusieurs fonctions, fonctionnalités, applications et /ou les communications réseau et les transactions réseau qui fonctionnent dans un serveur ou un appareil partagé. Les instances (locataires) sont logiquement isolées, mais physiquement intégrées. Le degré d'isolement logique doit être complet, mais le degré d'intégration physique variera.			

Critères Obligatoires

La réponse par écrit aux critères obligatoires suivants doit être soumise dans le cadre de la partie A du processus de présélection en soumettant le tableau ci-dessous, complété avec une auto-évaluation et une référence à l'endroit où se trouve la preuve justificative dans la réponse écrite. Les preuves peuvent inclure :

- Captures d'écran de la solution utilisée
- Extraits des spécifications techniques ou de la documentation du produit
- Manuel du produit
- Schémas d'architecture et de conception du système

Les critères obligatoires suivants doivent être satisfaits.

Table 2: Critères obligatoires

Critères obligatoires	**Auto-évaluation**		**Référence**
	Satisfait	**Non satisfait**	
M1 – Services de sécurité périmétrique infonuagique La solution doit fournir des services de sécurité périmétrique infonuagique. Le FEO de la solution proposé doit démontrer que les solutions SSBI fournissent la liste suivante de services de sécurité périmétrique : a) Pare-feu de nouvelle génération (NGFW) décrit comme un pare-feu de couche 4 à 7 qui autorise et refuse l'accès en fonction des adresses IP, des ports, des protocoles, de l'application, de l'identité, des groupes et des emplacements b) Secure Web Gateway (SWG) décrit comme le filtrage des logiciels malveillants et des logiciels malveillants du trafic Internet initié par l'utilisateur et applique la conformité à la politique pour le trafic Web, et empêche l'accès aux sites Web inacceptables et illégaux et aux sites Web connus pour contenir des menaces malveillantes et des virus c) Système de détection et de prévention des intrusions (IDPS) pour analyser le trafic décrypté des tentatives d'intrusion et bloquer les intrusions ; d) Advanced Threat Detection (ATD) qui identifie et bloque les logiciels malveillants intégrés dans les fichiers en transit et les fichiers contenant des logiciels malveillants, protégeant 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 ; e) Inspection SSL/TLS (Secure Sockets Layer, Transport Layer Security) qui déchiffre et inspecte le trafic SSL et TLS à la recherche de menaces, protégeant SPC contre les tentatives d'utilisation de code malveillant caché dans les flux de trafic chiffrés ; et f) Inspection SSH qui reconnaît les transferts de fichiers via SCP et SFTP, à inspecter par d'autres services de sécurité.			

Critères obligatoires	Auto-évaluation		Référence
	Satisfait	Non satisfait	
M2 - Capacité de mesure de l'expérience utilisateur La solution doit fournir une capacité de mesure historique de l'expérience utilisateur qui rend compte de l'expérience utilisateur et des tendances à l'aide d'une échelle d'évaluation. Une échelle d'évaluation est définie comme une échelle qualitative qui mesure l'expérience des utilisateurs de mauvaise à élever. Le FEO de la solution proposée doit démontrer la capacité de mesure de l'expérience utilisateur sous la forme de captures d'écran d'un tableau de bord ou d'un rapport qui inclut l'historique de l'expérience utilisateur et les tendances.			

Partie B – Réponse écrite cotée par points et session virtuelle interactive

Réponse écrite cotée par points

La réponse par écrit aux critères obligatoires suivants doit être soumise dans le cadre de la partie A du processus de présélection en soumettant le tableau ci-dessous, complété avec une auto-évaluation et une référence à l'endroit où se trouve la preuve justificative dans la réponse écrite. Les preuves peuvent inclure :

- Captures d'écran de la solution utilisée
- Extraits des spécifications techniques ou de la documentation du produit
- Manuel du produit
- Schémas d'architecture et de conception du système
- Copie des certifications

Tableau 3: Réponse écrite cotée par points

Réponse écrite cotée par points	**Attribution des points** **Note maximale = 43 points**	**Référence**
	Auto-évaluation	
WR1 : Déploiement SSBI sur site et basé sur l'infonuagique (3 points) Le FEO de la solution doit fournir la preuve que la solution SSBI proposée est capable de déployer une instance de la solution dans un emplacement physique déterminé par le Gouvernement du Canada (GC), comme un centre de données d'entreprise (EDC) du GC, géré par une plate-forme centralisée de gestion SSBI qui gère à la fois les déploiements SSBI sur site et dans un environnement SSBI basé sur l'infonuagique. Le FEO de la solution doit fournir des extraits des spécifications techniques du produit pour confirmer que la solution proposée peut être entièrement mise en œuvre dans un centre de données.	Les points seront attribués comme suit : • La preuve de cette capacité est démontrée = 3 points • La preuve de la capacité n'est pas suffisamment démontrée = 0 point **Auto-évaluation :**	

Réponse écrite cotée par points	**Attribution des points** **Note maximale = 43 points** **Auto-évaluation**	**Référence**
WR2 : Préparation au déploiement : processus d'évaluation du CCCS (10 points) Le FEO de la solution doit fournir la preuve que la solution SSBI proposée a terminé ou est en train de terminer le processus d'évaluation de la sécurité des technologies de l'information (TI) du fournisseur de services infonuagiques (CSP) du Centre canadien pour la cybersécurité (CCCS). (ITSM.50.100) (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux) Le FEO de la solution doit fournir une documentation du CCCS sous la forme d'une lettre, d'un courriel ou d'un rapport confirmant que le processus est terminé ou en cours.	Les points seront attribués comme suit : • La preuve est démontrée = 10 points • La preuve n'est pas démontrée = 0 point **Auto-évaluation :**	
R3 : Préparation à la sécurité (jusqu'à 10 points) Le FEO de la solution doit fournir la preuve que la solution SSBI proposée est en cours ou a obtenu les certifications d'un tiers partie indépendant répertoriées ci-dessous. Le FEO de la solution doit fournir la documentation de certification ou la confirmation du tiers que la certification est en cours pour chacun des éléments suivants. (a) ISO/IEC 27001:2013 Technologies de l'information -- Techniques de sécurité -- Systèmes de gestion de la sécurité de l'information – Certification obtenue par un organisme de certification accrédité. (b) ISO/IEC 27017:2015 Technologies de l'information -- Techniques de sécurité -- Code de pratique pour les contrôles de la sécurité de l'information basé sur ISO/IEC 27002 pour les services cloud réalisé par un organisme de certification accrédité. (c) ISO/IEC 27018:2014 Technologies de l'information -- Techniques de sécurité -- Code de pratique pour la protection des informations personnelles identifiables (PII) dans les nuages publics agissant en tant que processeurs de PII – Certification obtenue par un organisme de certification accrédité (d) 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.	Pour (a), (b) et (c), les points seront attribués comme suit pour chaque certification : • Avoir actuellement la certification = 2 points • Actuellement dans le processus de certification, mais pas terminé = 1 points • Non certifié et pas actuellement en cours de certification = 0 point **Auto-évaluation :** Pour (d), les points seront attribués comme suit : • Avoir actuellement la certification = 4 points • Actuellement dans le processus de certification, mais pas terminé = 2 points • Non certifié et pas actuellement en cours de certification = 0 point **Auto-évaluation :**	
WR4 : Intégration de la sécurité des terminaux (jusqu'à 3 points) Le FEO de la solution doit fournir la preuve que la solution peut automatiser les réponses aux menaces qui ont été identifiées par les produits de sécurité des terminaux suivants : a) McAfee ePO	Pour chaque produit de sécurité listé ci-dessus, les points seront attribués comme suit : • La capacité est démontrée = 1 point	

Réponse écrite cotée par points	**Attribution des points** **Note maximale = 43 points** **Auto-évaluation**	**Référence**
b) Windows Defender c) Cisco AMP pour les terminaux Les termes automatiser, atomiquement et automatique font référence à un processus ou à un évènement qui se déroule sans aucune intervention humaine. Le FEO de la solution doit fournir de la documentation comme des références aux manuels des produits et des captures des écrans de configuration de la solution pour confirmer que la solution proposée répond à cette exigence.	• La capacité n'est pas démontrée = 0 point **Auto-évaluation :**	
WR5 : Résidence des données (jusqu'à 10 points) Le FEO de la solution doit fournir la preuve que la solution SSBI est déployable dans un environnement où les données et les plans de contrôle de la solution résident au Canada. Le FEO de la solution doit fournir une documentation confirmant que la solution satisfait à cette exigence.	Les points seront attribués comme suit : • Le critère est démontré = 10 points • Le critère n'est pas démontré = 0 points **Auto-évaluation :**	
WR6 : Capacité d'isolation du navigateur distant (IND) (jusqu'à 4 points) Le FEO de la solution doit démontrer que la capacité IND de la solution peut autoriser ou refuser: a) les téléchargements de fichiers; b) les téléchargements de fichiers; c) les captures d'écran; et d) le copier-coller de toute information affichée. **La capacité d'isolation du navigateur distant** est définit comme une capacité IND native qui permet à l'activité de navigation Web d'un utilisateur d'être exécutée sur un serveur distant dans un environnement isolé, plutôt que sur l'ordinateur de l'utilisateur. RBI est hébergé dans l'environnement infonuagique des FEO de solution SSBI, protégeant les ordinateurs des utilisateurs contre les menaces Web, contenant les menaces pour l'environnement isolé. Le FEO de la solution doit fournir des extraits des spécifications techniques du produit, des manuels du produit ou des captures d'écran pour confirmer que la solution proposée répond à la capacité IND.	Pour chaque capacité répertoriée, des points seront attribués comme suit: • La capacité est démontrée = 1 point • La capacité n'est pas démontrée = 0 point **Auto-évaluation :**	

Réponse écrite cotée par points	**Attribution des points** **Note maximale = 43 points** **Auto-évaluation**	**Référence**
WR7 : accès à une application non Web (jusqu'à 3 points) Le FEO de la solution doit démontrer la capacité de la solution à fournir un accès sécurisé aux applications non Web pour les utilisateurs mobiles qui utilisent un appareil BYOD sans logiciel client CSS installé, via les fonctionnalités suivantes : a) protocole de bureau à distance (RDP); b) Secure Shell (SSH) ; et c) montage du système de fichiers à distance comme Server Message Block (SMB). Un application non basée sur le Web est un application accessible sans l'utilisation d'un navigateur Web et généralement exécutée sur l'ordinateur d'un utilisateur.	Les points seront attribués comme suit : • La fonctionnalité est démontrée = 1 point • La fonctionnalité n'est pas démontrée = 0 point **Auto-évaluation :**	

Critères cotés par points pour la session virtuelle interactive

Les FEOs de solution qui ont satisfait aux certifications et aux exigences obligatoires seront invités à une session virtuelle interactive de 75 minutes. Les critères cotés doivent être démontrés à l'aide de la solution réelle, soit dans un environnement de production ou de démonstration, en utilisant les mêmes versions logicielles que la solution de production.

Tableau 3 : Critères cotés par points – Session virtuelle interactive

	Note maximale = 20 Points
IR1	**Expérience utilisateur - Mesures de latence (jusqu'à 6 points)** Le FEO de la solution doit fournir la preuve que la solution est capable de fournir des mesures de latence saut par saut. Les preuves suivantes doivent être démontrées : • la latence de tous les sauts ; et • saute sur Internet du point de terminaison de l'utilisateur à la destination. Les points seront attribués comme suit pour chaque preuve : • La preuve est démontrée = 3 points • La preuve est partiellement démontrée (ne montrant pas tous les sauts) = 2 points • La preuve n'est pas démontrée = 0 point
IR2	**Expérience utilisateur - Temps de réponse de l'application (2 points)** Le FEO de la solution doit fournir la preuve que la solution peut déterminer la disponibilité et le temps de réponse des applications publiques et privées de destination afin de déterminer si l'application est responsable de la mauvaise expérience utilisateur. Les points seront attribués comme suit : • La capacité est démontrée = 2 points • La capacité n'est pas démontrée = 0 point

	Note maximale = 20 Points
IR3	**Courtier de sécurité d'accès au cloud (CNSA) (3 points)** Le FEO de la solution doit fournir la preuve que la solution dispose d'une capacité CASB native qui inclut: a) Prévention de la perte de données (DLP) ; b) Analyse du comportement des utilisateurs et des entités (UEBA) ; c) Conformité aux réglementations et aux politiques gouvernementales ; et d) Détection des menaces. Les points seront attribués comme suit : • Les quatre capacités énumérées sont démontrées = 3 points • Trois ou moins des capacités répertoriées ne sont pas démontrées = 0 point
IR4	**Gestion de la posture de sécurité infonuagique (PSI) (jusqu'à 3 points)** Le FEO de la solution doit fournir la preuve que la solution dispose d'une fonctionnalité PSI native qui : a) surveille, évalue et évalue la conformité à la sécurité et les violations réglementaires dans les environnements IaaS et PaaS ; et b) notifie 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 et automatise leur correction. Les points seront attribués comme suit : • Les deux capacités listées sont démontrées = 3 points • Une ou moins des capacités sont démontrées = 0 points
IR5	**Gestion de la posture de sécurité SaaS (GPSS) (jusqu'à 3 points)** La solution doit fournir la preuve que la solution dispose d'une fonctionnalité SSPM native qui : a) surveille et détecte les paramètres qui introduisent des risques de sécurité dans les environnements SaaS ; b) fournir des alertes en cas de mauvaise configuration ; et c) automatise ou fournit une correction guidée pour résoudre les risques. Les points seront attribués comme suit : • Les trois capacités listées sont démontrées = 3 points • Deux ou moins des capacités répertoriées ne sont pas démontrées = 0 point
IR6	**Découverte automatique des applications (3 points)** Le FEO de la solution doit démontrer la capacité de la solution à : a) découvrir, identifier et afficher automatiquement les applications à l'intérieur de l'interface de gestion du SSBI qui sont demandées et consultées par les utilisateurs ou appareils SSBI, sans avoir à importer de registre ; et b) permettre aux administrateurs SSBI d'appliquer directement des politiques d'accès à ces applications via l'interface de gestion du SSBI après que l'application a été automatiquement découverte et identifiée. Les points seront attribués comme suit : • Les deux capacités listées sont démontrées = 3 points • Une ou moins des capacités répertoriées ne sont pas démontrées = 0 point