Form 4 - Cloud SCI Controls

Immigration, Refugees and Citizenship Canada
Immigration, Réfugiés et Citoyenneté Canada

Canada

Introduction

In order to properly assess a Cloud Service, the following authenticated and certified information must be provided for our Cyber Security control and assessment to ascertain coherence to Supply Chain Integrity:

Control Domain	Response	(document / page / paragraph)
Company's legal registered name		
Company's HQ geo location		
Company's detailed ownership structure		
Company's 3 year audited Financial (income statement, Cash flow, and balance sheet) prospectus		
DBRS, SEDAR, and CRA Company profile		
Number of past, ongoing, and potential upcoming litigations and size		
Outstanding "off book" high ratio loans, hidden investments, and write-offs in the past 5 years		

Company Sub-processors

Sub-processors are entities that provide the infrastructure on which the SaaS services run; the entities that support specific SaaS services which may require them to process customer data; and third parties with whom the SaaS provider has contracted to provide processing activities for specific SaaS services.

For each sub-processor please provide the following information with evidence authenticating your claim:

Control Domain	Response	(document name / page / paragraph)
Company's Geolocation	Geolocation within countries with like-minded intelligence services.	

Company's software development locations	Has the software been thoroughly checked for potential backdoor entry?	
Location where Information is Processed	(for example, usage statistics or administrative data)	
Data Residency	Does all data remain in Canada?	

Ownership assessment should be considered for each sub-processor who can access, store, or process client information. Please list the following information with evidence authenticating your claim:

Sub-Processor	Purpose of Processing	Information Processed	Data Residency
Supplier 1			
Supplier 2			
Data Center Ownership 1			
Data Center Ownership 2			
3rd party development			
3rd party testing services			
3rd party service desk			

Technical Assessment Definitions

Below are the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) controls for Supply Chain Management, Transparency, and Accountability from the Consensus Assessments Initiative Questionnaire v3.1:

Control Domain	Control ID	Definition of Control Specification
Data Quality and Integrity	STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.
Incident Reporting	STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).
Network / Infrastructure Services	STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.
Provider Internal Assessments	STA-04	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.

Control Domain	Control ID	Definition of Control Specification
Supply Chain Governance Reviews	STA-06	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.
Supply Chain Metrics	STA-07	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.
Third Party Assessment	STA-08	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.
Third Party Audits	STA-09	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.

Technical Assessment Responses

To ensure the controls above have been met, evidence of compliance with the following assessment questions should be shown and document name, page number, and paragraph provided from your RFP:

Question ID	Consensus Assessment Questions	Compliant (Y/N)	Reference to third party audit (report/page/paragraph)
STA-01.1	Do you **inspect** and **account for data quality errors** and associated risks, and work with your cloud supply-chain partners to correct them?		
STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper **separation of duties**, **role-based access**, and **least-privileged access** for all personnel within your supply chain?		
STA-02.1	Do you **make security incident information available** to all affected customers and providers periodically through electronic methods (**e.g., portals**)?		
STA-03.1	Do you **collect capacity** and use data for all relevant components of your cloud service offering?		
STA-03.2	Do you **provide tenants** with **capacity planning and use reports?**		

Question ID	Consensus Assessment Questions	Compliant (Y/N)	Reference to third party audit (report/page/paragraph)
STA-04.1	Do you **perform annual internal assessments** of conformance and effectiveness of your **policies, procedures, and supporting measures and metrics**?		
STA-05.1	Do you **select and monitor outsourced providers** in compliance **with laws in the country where the data is processed, stored, and transmitted?**		
STA-05.2	Do you **select and monitor** outsourced providers in compliance with **laws in the country where the data originates?**		
STA-05.3	Does **legal counsel review** all **third-party agreements**?		
STA-05.4	Do third-party agreements include **provision for the security and protection of information and assets?**		
STA-05.5	Do you provide the client with a list and **copies of all sub-processing agreements and keep this updated?**		
STA-06.1	Do you review the risk management and governance processes of partners to account for **risks inherited from other members of that partner's supply chain?**		
STA-07.1	**Are policies and procedures established,** and supporting business processes and technical measures implemented, for maintaining complete, accurate and **relevant agreements (e.g., SLAs) between providers and customers (tenants)**?		
STA-07.2	Do you have the **ability to measure and address non-conformance of provisions and/or terms across the entire supply chain** (upstream/downstream)?		
STA-07.3	**Can you manage** service-level **conflicts or inconsistencies** resulting from disparate **supplier relationships?**		
STA-07.4	Do you r**eview all agreements, policies and processes at least annually?**		
STA-08.1	Do you assure reasonable information security across your information supply chain by performing an **annual review**?		
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?		

Question ID	Consensus Assessment Questions	Compliant (Y/N)	Reference to third party audit (report/page/paragraph)
STA-09.1	Do you permit tenants to perform independent vulnerability assessments?		
STA-09.2	Do you have external third-party services conduct vulnerability scans and periodic penetration tests on your applications and networks?		

** If you need to submit additional auditable documentation and certification, please attach them with your response email.

Authentication and Authorization of information provided

Please provide the following information to certify that all information provided are authenticated and audited information:

| --- | --- | --- | --- |
| Name of Official | Date | Company | Official's Authority |

Signature

Formulaire 4 -Contrôles visant l'ICA des services infonuagiques

Introduction

Pour évaluer adéquatement un service infonuagique, les renseignements vérifiés et certifiés suivants doivent être fournis afin de veiller à ce que l'équipe de cybersécurité effectue le contrôle et l'évaluation dans le but d'assurer la cohérence de l'intégrité de la chaîne d'approvisionnement (ICA).

Domaine de contrôle	Réponse	(Document / page / paragraphe)
Dénomination sociale de l'entreprise enregistrée		
Géolocalisation du siège social de l'entreprise		
Structure détaillée du capital de l'entreprise		
Prospectus financier triennal vérifié de l'entreprise (relevé des gains, flux de trésorerie et bilan)		
Profil de l'entreprise du DBRS, du SEDAR et de l'ARC		
Nombre de litiges antérieurs, en cours et potentiellement à venir, et ampleur de ceux-ci		
Prêts à ratio élevé « hors livres » actifs, investissements cachés et radiations au cours des cinq dernières années		

Sous-traitants de l'entreprise

Les sous-traitants sont des entités qui fournissent l'infrastructure dans laquelle les services de logiciel-service (SaaS) sont exécutés, des entités qui appuient des services particuliers de SaaS, ce qui leur demande potentiellement de traiter des données de clients, et des tierces parties dont le fournisseur de SaaS a retenu les services pour offrir des activités de traitement dans le cadre de services particuliers de SaaS.

Pour chaque sous-traitant, veuillez indiquer les renseignements suivants ainsi que les données probantes attestant votre affirmation.

Domaine de contrôle	Réponse	(Nom du document / page / paragraphe)
Géolocalisation de l'entreprise	Géolocalisation au sein de pays ayant des services de renseignement aux vues similaires.	
Lieux de développement des logiciels de l'entreprise	Le logiciel a-t-il fait l'objet d'une vérification approfondie visant l'entrée par un moyen détourné potentiel?	
Lieu de traitement de l'information	(Par exemple, statistiques concernant l'usage ou données administratives)	
Hébergement des données	Les données demeurent-elles toutes au Canada?	

Il faudrait envisager la réalisation d'une évaluation de la propriété de chaque sous-traitant qui pourrait entreposer ou traiter des renseignements sur les clients, ou y avoir accès. Veuillez dresser la liste des renseignements suivants en indiquant des données probantes attestant votre affirmation.

Sous-traitant	But du traitement	Renseignements traités	Hébergement des données
Fournisseur 1			
Fournisseur 2			
Propriété du centre de données 1			
Propriété du centre de données 2			
Développement par une tierce partie			
Services de mise à l'essai par une tierce partie			
Bureau de service d'une tierce partie			

Définitions de l'évaluation technique

Vous trouverez ci-après les contrôles de la matrice de contrôle des services infonuagiques (MCSI) de la Cloud Security Alliance (CSA) visant la gestion de la chaîne d'approvisionnement, la transparence et la responsabilisation, tirés de la version 3.1 du questionnaire de l'initiative d'évaluation par consensus.

Domaine de contrôle	Code de contrôle	Définition de la spécification du contrôle
Qualité et intégrité des données	STA-01	Les fournisseurs doivent inspecter les erreurs liées à la qualité des données et les risques connexes, en rendre compte, et collaborer avec leurs partenaires de la chaîne d'approvisionnement de l'informatique en nuage afin de les corriger. Les fournisseurs doivent concevoir et mettre en œuvre des mesures de contrôle afin d'atténuer et de maîtriser les risques relatifs à la sécurité des données par une séparation appropriée des tâches, un accès fondé sur le rôle et un accès fondé sur le droit d'accès minimal pour tout le personnel de la chaîne d'approvisionnement.
Signalement des incidents	STA-02	Le fournisseur doit mettre tous les renseignements sur les incidents de sécurité à la disposition de l'ensemble des clients et des fournisseurs touchés, et ce, périodiquement par voie électronique (p. ex. à l'aide de portails).
Services d'infrastructure et de réseau	STA-03	Il faut concevoir, élaborer et déployer les interfaces système-systèmes (API) et les applications (physiques et virtuelles) essentielles aux activités ou ayant une incidence sur les clients (locataires) et leurs configurations, et les éléments du réseau et des systèmes de l'infrastructure, conformément aux attentes établies d'un commun accord quant au niveau de service et de capacité, ainsi qu'aux politiques et aux procédures de gouvernance des TI et de gestion des services.
Évaluations internes du fournisseur	STA-04	Chaque année, le fournisseur doit mener des évaluations internes du respect et de l'efficacité de ses politiques, de ses procédures et des mesures à l'appui.
Examen de la gouvernance de la chaîne d'approvisionnement	STA-06	Les fournisseurs doivent examiner les processus de gouvernance et de gestion des risques de leurs partenaires afin de s'assurer que les pratiques sont uniformes et qu'elles tiennent compte des risques provenant des autres membres de la chaîne d'approvisionnement de l'informatique en nuage de ces partenaires.
Paramètres de la chaîne d'approvisionnement	STA-07	Des politiques et des procédures doivent être mises en œuvre pour assurer un examen uniforme des ententes de services (p. ex. accords sur les niveaux de service) entre les fournisseurs et les clients (locataires) à l'échelle de la chaîne d'approvisionnement pertinente (en aval et en amont). Il faut effectuer un examen au moins chaque année afin de cibler les problèmes de non-conformité dans les ententes établies. Les examens devraient donner lieu à la prise de mesures pour corriger les conflits ou les divergences attribuables aux relations disparates avec les fournisseurs.
Évaluation par un tiers	STA-08	Les fournisseurs doivent assurer une sécurité raisonnable des renseignements à l'échelle de la chaîne d'approvisionnement de leurs renseignements en procédant à un examen annuel. L'examen doit viser tous les partenaires et les fournisseurs tiers dont dépend la chaîne d'approvisionnement des renseignements.

Domaine de contrôle	Code de contrôle	Définition de la spécification du contrôle
Vérifications par des tiers	STA-09	Les fournisseurs de services tiers doivent démontrer leur conformité à la sécurité et à la confidentialité de l'information, au contrôle de l'accès, aux définitions de service et aux accords sur le niveau de prestation compris dans les contrats conclus avec des tiers. Les rapports, les dossiers et les services de tiers doivent faire l'objet d'une vérification et d'un examen au moins chaque année dans le but de régir et de maintenir la conformité avec les accords sur la prestation de services.

Réponses à l'évaluation technique

Pour veiller à ce que les contrôles susmentionnés aient été respectés, il faut fournir une preuve de conformité aux questions d'évaluation suivantes et indiquer le nom du document, le numéro de page et le paragraphe de votre DP.

N° de la question	Questions de l'évaluation par consensus	Conformité (O/N)	Référence à une vérification réalisée par un tiers (rapport/page/paragraphe)
STA-01.1	Procédez-vous à l'**inspection des erreurs liées à la qualité des données** et les risques connexes et en **rendez-vous compte**, et collaborez-vous avec vos partenaires de la chaîne d'approvisionnement de l'informatique en nuage afin de les corriger?		
STA-01.2	Concevez-vous et mettez-vous en œuvre des mesures de contrôle afin d'atténuer et de maîtriser les risques relatifs à la sécurité des données par une **séparation** appropriée **des tâches**, un **accès fondé sur le rôle** et un **accès fondé sur le droit d'accès minimal** pour tout le personnel de la chaîne d'approvisionnement?		
STA-02.1	**Mettez-vous tous les renseignements sur les incidents de sécurité à la disposition** de l'ensemble des clients et des fournisseurs touchés, et ce, périodiquement par voie électronique (**p. ex. à l'aide de portails**)?		
STA-03.1	**Recueillez-vous des données** sur la capacité et l'usage pour tous les éléments pertinents des services infonuagiques que vous offrez?		
STA-03.2	**Fournissez-vous** aux **locataires des rapports sur la planification de la capacité et sur l'usage?**		

N° de la question	Questions de l'évaluation par consensus	Conformité (O/N)	Référence à une vérification réalisée par un tiers (rapport/page/paragraphe)
STA-04.1	**Menez-vous des évaluations internes annuelles** du respect et de l'efficacité de vos **politiques**, de vos **procédures** et de vos **mesures à l'appui**?		
STA-05.1	**Sélectionnez-vous** des fournisseurs externes **et assurez-vous leur surveillance** conformément aux **lois dans le pays où les données sont traitées, entreposées et transmises?**		
STA-05.2	**Sélectionnez-vous** des fournisseurs externes **et assurez-vous leur surveillance** conformément aux **lois dans le pays d'origine des données?**		
STA-05.3	Un **conseiller juridique examine-t-il** toutes les **ententes conclues avec une tierce partie**?		
STA-05.4	Les ententes conclues avec une tierce partie comprennent-elles une **disposition concernant la sécurité et la protection des renseignements et des biens?**		
STA-05.5	Fournissez-vous au client une liste et des **copies de toutes les ententes de sous-traitance et les tenez-vous à jour?**		
STA-06.1	Examinez-vous les processus de gestion et de gouvernance des risques des partenaires afin de tenir compte des **risques provenant des autres membres de la chaîne d'approvisionnement de ces partenaires?**		
STA-07.1	**Des politiques et des procédures sont-elles établies,** et les processus opérationnels et mesures techniques à l'appui sont-ils mis en œuvre dans le but de tenir à jour des **ententes** complètes, exactes et **pertinentes (p. ex. ANS) entre les fournisseurs et les clients (locataires)**?		
STA-07.2	Disposez-vous de la **capacité d'évaluer la non-conformité aux dispositions ou aux conditions à l'échelle de la chaîne d'approvisionnement** (en amont / en aval), **et de remédier à ces cas**?		

N° de la question	Questions de l'évaluation par consensus	Conformité (O/N)	Référence à une vérification réalisée par un tiers (rapport/page/paragraphe)
STA-07.3	**Pouvez-vous gérer les conflits ou les incohérences** au niveau du service découlant de **relations** disparates avec les **fournisseurs?**		
STA-07.4	**Examinez-vous la totalité des ententes, des politiques et des processus au moins toutes les années?**		
STA-08.1	Assurez-vous une sécurité raisonnable des renseignements à l'échelle de la chaîne d'approvisionnement de vos renseignements en procédant à un **examen annuel**?		
STA-08.2	Votre examen annuel vise-t-il tous les partenaires et fournisseurs tiers dont dépend votre chaîne d'approvisionnement de renseignements?		
STA-09.1	Permettez-vous aux locataires d'effectuer des évaluations indépendantes de la vulnérabilité?		
STA-09.2	Disposez-vous de services de tiers externes qui procèdent à des analyses de la vulnérabilité et à des essais de pénétration périodiques visant vos applications et vos réseaux?		

** Si vous devez soumettre des documents et des certificats vérifiables supplémentaires, veuillez les joindre à votre courriel de réponse.

Attestation et autorisation des renseignements fournis

Veuillez fournir l'information suivante pour garantir que les renseignements fournis sont bien vérifiés et certifiés :

| --- | --- | --- | --- |
| Nom du(de la) représentant(e) | Date | Entreprise | Titre du(de la) représentant(e) |

Signature