SHARED SERVICES CANADA

Invitation to Qualify for
Government of Canada Cloud Service Procurement Vehicle
(GC Cloud)

ANNEX A, APPENDIX 2 – QUALIFICATION REQUIREMENTS FOR STREAM 2

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
General Requirements			
M1	General	The Respondent must identify the existing Cloud Service Provider (CSP), who's Commercially Available Cloud Services will be offered to Canada at the solicitation stage of this procurement process.	Identify the proposed Commercially Available Cloud Service: _____ Identify the Cloud Service Provider (CSP) for the proposed Commercially Available Cloud Service: _____
M2	General	The Respondent must confirm that they are either : a) the Cloud Service Provider for the proposed Commercially Available Cloud Services identified in M1; **OR** b) an Alternative Service Provider who is: (i) authorized by the Cloud Service Provider to proposed Commercially Available Cloud Services identified in M1; and (ii) capable of providing Canada all Commercially Available Cloud Services of the proposed Cloud Service Provider identified in M1. **OR**	**If the Respondent is the Cloud Service Provider:** • No demonstration of compliance is required for M2. **If the Respondent is not the Cloud Service Provider and is considered either an Alternative Service Provider or a Cloud Reseller:** • The Respondent must provide a signed statement from the Cloud Service provider on their corporate letterhead that confirms: a) The Respondent is an authorized provider of the Commercially Available Cloud Services offered by the CSP identified in M1; and b) The Respondent is capable of providing all Commercially Available Cloud Services of the proposed CSP identified in M1.

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
		c) a Cloud Reseller who is: (i) authorized by the Cloud Service Provider to proposed Commercially Available Cloud Services identified in M1; and (ii) capable of providing Canada access to all Commercially Available Cloud Services of the proposed Cloud Service Provider identified in M1. **Please note** – For item (c) (ii) listed above, the word "access" is defined in accordance with NIST SP800-32 which states "Ability to make use of any information system (IS) resource"	
M3	General	The Cloud Service Provider identified in M1 must provide Commercially Available Cloud Services.	The Respondent must demonstrate compliance by providing documentation outlining the services available in the proposed Commercially Available Cloud Services identified in M1. The substantiation required for M3 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M4	General	The Cloud Service Provider of the proposed Commercially Available Cloud Service must provide pricing for services, billing and support in Canadian dollars including but not limited to consumption reporting.	The Respondent must demonstrate compliance by providing documentation outlining examples that demonstrate the proposed Commercially Available Cloud Service's ability to provide pricing (in Canadian dollars) for services, billing and support including but not limited to consumption reporting. To be considered compliant, the provided documentation must include: a) Screen captures or system documentation detailing and outlining how the services will be priced, billed and supported in CDN dollars. The substantiation required for M4 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Cloud Service meets the requirement.

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
			Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M5	General	The proposed Commercially Available Cloud Services must have published service level agreements (SLA) available to its customers. The service level commitments (detailed in the published service level agreements) must provide commercial clients support that includes, at the minimum, any published and Commercially Available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the Cloud Service Provider's Commercially Available Cloud Services.	The Respondent must demonstrate compliance by providing documentation that outline's the Cloud Service Provider's published service level agreements and commitments for the proposed Commercially Available Cloud Services. To be considered compliant, the provided documentation must include: a) Screen shots or documentation of the published service level agreements detailing any published and Commercially Available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the Cloud Service Provider's Commercially Available Cloud Services including but not limited to the service commitment, credit process and monthly uptime percentage. The substantiation required for M5 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
M6	General	The Cloud Service Provider of the proposed Commercially Available Cloud Service must provide the ability for the consumer to choose the official language of their choice, French or English, when browsing, ordering and contacting the Cloud Service Provider.	The Respondent must demonstrate how the proposed Commercially Available Cloud Service provides the capability to allow consumers to choose which official language, French or English. To be considered compliant, the provided documentation needs to demonstrate the Commercially Available Cloud Service's ability to perform the following in both French or English: a) browsing the service(s) on their website(s); b) ordering services on their website(s); c) contacting the company for assistance via phone, email or chat. The substantiation required for M6 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. a) Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
Data Center Facilities Requirements			
M7	Data Center Facilities	The Cloud Service Provider of the proposed Commercially Available Cloud Service must implement security measures that ensure the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. This includes, at a minimum a) sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; b) proper handling of IT media; c) controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability; d) controlled access to information system output devices to prevent unauthorized access to Canada's data; e) limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification; f) escorting visitors and monitoring visitor activity; g) maintaining audit logs of physical access; h) controlling and managing physical access devices; i) enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites); and j) recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.	The Respondent must provide documentation that demonstrates how the Cloud Service Provider of the proposed Commercially Available Cloud Service complies with the requirements in M7. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are used to ensure the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. The substantiation required for M7 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
Personnel Security Requirements			
M8	Personnel Security	The Cloud Service Provider of the proposed Commercially Available Cloud Services must implement security measures that grant and maintain the required level of security screening for the Cloud Service Provider and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. 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. This includes, at a minimum: a) description of the employee and subcontractor positions that require access to Canada's Data or have the ability to affect the confidentiality, integrity or availability of the Services; b) process for ensuring that employees and contractors understand, are aware, and fulfil, their responsibilities for information security, and are suitable for the roles for which they are considered; c) process for security awareness and training as part of employment onboarding and when employee and subcontractor roles change; d) process that is enforced when an employee or subcontractor changes their role or when employment is terminated; and e) approach for detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of cloud services hosting GC assets and data	The Respondent must provide documentation that demonstrates how the Cloud Service Provider of the proposed Commercially Available Cloud Service complies with the requirements in M8. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, process and procedures that are used to grant and maintain the required level of security screening for the Cloud Service Provider and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. The substantiation required for M8 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Cloud Service Provider of the proposed Commercially Available Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
Third Party Assurance Requirements			
M9	Third Party Assurance	The Cloud Service Provider must be designed and developed to ensure the security of their proposed Commercially Available Cloud Service, including, implementing information security policies, procedures, and security controls.	The Respondent must provide documentation that demonstrates how the Cloud Service Provider of the proposed Commercially Available Cloud Service complies with the requirements in M9. Compliance must be demonstrated by providing one or more of the following industry certifications identified below, and validated through independent third party assessments. a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements, **OR** AICPA Service Organization Control (SOC) 2 Type II **AND** b) Self-assessment of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version. The ISO27001 certification or assessment report and AICPA SOC2 Type II must: a) Identify the legal business name of the proposed CSP; b) Identify the current certification date and/or status; c) The scope of the report must map to locations and services offered by the proposed Commercially Available Cloud Service. 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; d) Be valid for the duration of the contract; e) Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality management system standard; and f) have been issued within the 12 months prior to the bidding closing date.

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
Data Protection Requirements			
M10	Data Protection	The physical locations of the proposed Commercially Available Cloud Service (which may contain Canada's data) must be located in either: a) A country within the North Atlantic Treaty Organization (NATO); b) A country within the European Union (EU); or c) A country with which Canada has an international bilateral industrial security instrument **Please note** - The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.	The Respondent must provide documentation that demonstrates how the proposed Commercially Available Cloud Service (identified in M1) meets the mandatory requirement outlined in M10. To be considered compliant, the provided documentation must include: a) an up-to-date (as of ITQ closing date) list of the physical locations (including city and country) for each data centre that may contain Canada's data including in backups or for redundancy purposes. The substantiation required for M10 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Cloud Service Provider meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.
Supply Chain Risk Management Requirements			
M11	Supply Chain Management	The Respondent must provide a third party supplier list containing information on any third parties (e.g. subsidiaries, subcontractors, etc.) that would provide Canada with the proposed Commercially Available Cloud Service. For the purposes of this requirement, a company who is merely a supplier of goods to the Cloud Service Provider of the proposed Commercially Available Cloud Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Cloud Service, is not considered to be a third party. Third party examples would include, for example, technicians who might be deployed or maintain the Commercially Available Cloud Services of the Cloud Service Provider that have been proposed by the Respondent in M1.	The Respondent must provide documentation that lists information on any third parties that could be used to perform any part of the supply chain that would provide Canada with the proposed Commercially Available Cloud Service whether they would be (i) subcontractors to the Respondent or Cloud Service Provider, or (ii) subcontractors to subcontractors of the Respondent or Cloud Service Provider down the chain, or (iii) any subsidiaries. The list must include at a minimum: a) The name of the third party; b) The address of the third party headquarters; c) The portion of the Work that would be performed by the third party; d) The location(s) where the third-party would provide Canada with the proposed Commercially Available Cloud Service.

Mandatory ID	Sub-Category	Requirement	Stream 2 - Required to demonstrate compliance with Tier 1 Assurance (Low Impact) (Up to and including Protected A Data)
		Please note: Respondents are advised that subsequent procurement phases may require the Respondent to notify Canada regularly when there are updates to the list of third party suppliers.	e) Any third party that could have access to Canada's data in the proposed Commercially Available Cloud Service. If the Cloud Service Provider of the proposed Commercially Available Cloud Service does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Cloud Service, the Respondent is requested to indicate this in their response to this requirement.
M12	Supply Chain Risk Management	The Cloud Service Provider of the proposed Commercially Available Cloud Service (identified in M1) must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within the supply chain.	The Respondent must demonstrate how the Cloud Service Provider of the proposed Commercially Available Cloud Service complies with the requirements in M12 as documented under the Cloud Service Provider Information Technology Security Assessment program. To be considered compliant, the provided documentation demonstrating compliance by providing at least one of the following three options: 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); **OR** 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; **OR** 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Cloud Service Provider's approach to SCRM and demonstrate how the Cloud Service Provider of the proposed Commercially Available Cloud Service will reduce and mitigate supply chain risks