SHARED SERVICES CANADA

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

ANNEX A, APPENDIX 1 – QUALIFICATION REQUIREMENTS FOR STREAM 1

Mandatory ID	Sub-Category	Requirement	Stream 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
General Requirements			
M1	General	The Respondent must identify itself as the 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 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 M2 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 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
M3	General	The proposed Commercially Available Cloud Service must provide the GC the ability to isolate data in Canada in an approved data center. For the purposes of this solicitation, an Approved Data Centre is defined as the following: a) The data center must be geographically located in Canada; and b) The data centre must meet all security requirements and certifications outlined in M8	The Respondent must demonstrate compliance by providing documentation outlining proposed Commercially Available Cloud Service's ability to isolate data in Canada in an approved data center. To be considered compliant, the provided documentation must include the following: a) Screen shots of the available data center where Canadian data centers are on the availability list; and b) a list or map indicating where geographically the data centers are located in Canada.; 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 have the ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. This includes ensuring that credentials remain within the geographic boundaries of Canada.	The Respondent must demonstrate compliance by providing documentation outlining the Cloud Service Provider's ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. To be considered compliant, the provided documentation must include: a) System documentation or white paper that outlines the policies, processes and procedures used to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. The substantiation required for M4 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

Mandatory ID	Sub-Category	Requirement	Stream 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
			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 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 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.
M6	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:

Mandatory ID	Sub-Category	Requirement	Stream 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
			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 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. 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.
M7	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 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

Mandatory ID	Sub-Category	Requirement	Stream 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
			Response the reference material can be found, including the title of the document, and the page and paragraph numbers.
Data Center Facilities Requirements			
M8	Data Center Facilities	The Cloud Service Provider of the proposed Commercially Available Cloud Service must ensure that security measures are implemented for 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. Physical protection measures must be applied in accordance with, or use an adequate risk-based approach aligned with the physical and environmental protection (PE), maintenance (MA), and media protection (MP) security controls outlined in the GC Security Control Profile for Cloud-Based GC IT Services for PBMM and the practices in the Royal Canadian Mounted Police (RCMP) guidance and standards on 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 M8. 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 implemented for 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 M8 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 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
Personnel Security Requirements			
M9	Personnel Security	The Cloud Service Provider of the proposed Commercially Available Cloud Service must implement security measures that grant and maintain the required level of security screening for the Cloud Service Provider's 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 M9. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including the policies, processes and procedures that are used to grant and maintain the required level of security screening for the Cloud Service Provider's 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 M9 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.
Third Party Assurance Requirements			
M10	Third Party Assurance	The Cloud Service Provider of the proposed Commercially Available Cloud Service 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 Cloud Service Provider of the proposed Commercially Available Cloud Service must also comply with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B,	The Respondent must demonstrate how the Cloud Service Provider of the proposed Commercially Available Cloud Service complies with the requirements in M10. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments.

Mandatory ID	Sub-Category	Requirement	Stream 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
		Medium Integrity and Medium Availability (PBMM) for the scope of the proposed Commercially Available Cloud Service provided by the Cloud Service Provider.	The Respondent must provide the following industry certifications to demonstrate compliance: a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements b) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services; and c) AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality. Each certification or assessment report 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. The Respondent can provide additional supplementary evidence from system security plans, information system design, information system architecture, or documents that provide a comprehensive system description, such as FedRAMP Moderate Certification Evidence or assessment of its Services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version, to support the claims from the above certifications, in order to demonstrate compliance to the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM).

Mandatory ID	Sub-Category	Requirement	Stream 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
Data Protection Requirements			
M11	Data Protection	The Cloud Service Provider of the proposed Commercially Available Cloud Services must have the ability for the GC to store and protect its information at rest, including data in backups or maintained for redundancy purposes within the geographic boundaries of Canada. This includes: a) identifying and providing the GC with an up-to-date list of the physical locations including city which may contain Canada's data in Canada for each data centre that will be used to provide the Services included in this contract. b) Identifying which portions of the Services are delivered from outside of Canada including all locations where data is stored and processed and where they manage the service from. c) ensuring the infeasibility of finding a specific customer's data on physical media; and d) employing encryption to ensure that no data is written to disk in an unencrypted form. **Please note:** Respondents are advised that subsequent procurement phases may require the Respondent and/or Cloud Service Provider of the proposed Commercially Available Cloud Service to notify Canada when there are updates to the list of physical locations which may contain Canada's data.	The Respondent must provide documentation that demonstrates how the Cloud Service Provider of the proposed Commercially Available Cloud Service (identified in M1) meets the mandatory requirement outlined in M11. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the policies, process and procedures that are used to store and protect its information at rest, including data in backups or maintained for redundancy purposes within the geographic boundaries of Canada; and b) For the portions of Services that could be delivered from outside of Canada, the Respondent must describe how Cloud Service Provider of the proposed Commercially Available Cloud Service will ensure Canada's data remains protected from unauthorized access, use, disclosure, modification, disposal, transmission, or destruction. The substantiation required for M11 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.

Mandatory ID	Sub-Category	Requirement	Stream 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
Supply Chain Risk Management Requirements			
M12	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. **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.	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. e) Any third party that could have access to Canada's data in the proposed Commercially Available Cloud Service. If the Cloud Service Provider 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.
M13	Supply Chain Risk Management	The Cloud Service Provider of the proposed Commercially Available Cloud Services must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide 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 M13 as documented under the Cloud Service Provider Information Technology Security Assessment program. To be considered compliant, the provided documentation must demonstrate that the CSP's supply chain risk management approach aligns with one of the following best practices 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); **OR**

Mandatory ID	Sub-Category	Requirement	Stream 1 - Required to demonstrate compliance with Tier 2 Assurance (Moderate Impact) (Up to and including Protected B Data)
			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.
Privacy Requirements			
M14	Privacy	The Cloud Service Provider of the proposed Commercially Available Cloud Service must demonstrate that it is compliant with the privacy policies, procedures, and provisions that meet the following industry certification: a) ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors **Please note:** Respondents are advised that subsequent procurement phases may require the Respondent to confirm to Canada on a regular basis that the proposed Commercially Available Cloud Service meets the above certification, and that the certification is valid for the duration of the contract.	To demonstrate compliance to the certification, the Respondent must provide: a) A copy of the Cloud Service Provider's most recent and ISO 27018 certification documents, which must have been issued within the 12 months prior to the solicitation closing date; and b) A copy of the ISO 27018 assessment report for their current Commercially Available Cloud Services.