APPENDIX M – Tier 2 Security Requirements

Security Requirements for Software as a Service

QUALIFICATION REQUIREMENTS

The following twenty (20) Security requirements must be met in order to demonstrate compliance with Tier 2 Assurance **(Up to and including Protected B Data).**

1. Tier 2 Assurance (Up to and including Protected B Data).

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M1	**Roles and Responsibilities for Security**	The Supplier must clearly delineate the roles and responsibilities for the security controls and features of the Services between the Supplier (any Supplier Sub-processors, as applicable) and Canada.	In the document, the Supplier must include, at a minimum, the parties' roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system backup; (iv) incident management; (v) System monitoring; and (vi) vulnerability management.
M2	**Master / Root Account Management**	The Supplier of the proposed Commercially Available Software as a 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 Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. 1) To be considered compliant, the provided documentation must include: 2) 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. 3) The substantiation required for the Master / Root Account Management, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
			proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

M3	**Data Protection Isolation**	The proposed Services 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) A data center that is geographically located in Canada; and b) A data centre that meets all security requirements and certifications identified. Data Center Facilities Requirements: The Supplier of the proposed Commercially Available Software as a Service must ensure that security measures are implemented for the protection of IT facilities and information system assets on which Canada 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 ITSG-33 Government of Canada 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;	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Data Center Facilities Requirements 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 Data Center Facilities Requirements - , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		i) enforcing safeguarding measures for Canada 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.	
M4	**Data Segregation**	The Supplier must, for both Tiers, implement controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Supplier's Service's and Supplier Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support: (a) The separation between Supplier's internal administration from resources used by its customers; and (b) The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M5	**Data Protection**	The Supplier of the proposed Commercially Available Software as a Services must have the ability or the Government of Canada 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 Government of Canada with an up-to-date list of physical locations including city which may contain Canada's data in Canada for each data centre that will be used to provide Services. 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 a disk in an unencrypted form. Suppliers please note: Suppliers are advised that subsequent procurement Streams may require the Supplier of the proposed Commercially Available Software as a Service to notify Canada when there are updates to the list of physical locations which may contain Canada's data.	The Supplier must demonstrate compliance by providing documentation outlining proposed Commercially Available Software as a 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 this criteria cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M6	**Data Center Facilities**	The Supplier of the proposed Commercially Available Software as a 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 aligned with the physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329) . The security measures required under this include, 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;	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Data Center Facilities Requirements. 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 Canada 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 Data Center Facilities Requirements, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		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.	Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M7	**Personnel Security**	The Supplier of the proposed Commercially Available Software as a Services must implement security measures that grant and maintain the required level of security screening for its respective personnel, as well as the personnel of any 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 Personnel Security) 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	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Personnel Security Requirements. 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 Supplier and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. The substantiation required in the Personnel Security Requirements, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		information security, and are suitable for the roles for which they are considered; c) process for security awareness and training as part of employment on boarding 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 effect on the reliability of cloud services hosting GC assets and data	Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M8	**Third Party Assurance**	The Supplier of the proposed Commercially Available Software as a Service must be designed and developed to ensure the security of their proposed Commercially Available Software as a Service, including, implementing information security policies, procedures, and security controls. The Supplier of the proposed Commercially Available Software as a Service must also comply with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM) for the scope of the proposed Commercially Available Software as a Service provided. Compliance will be validated and verified through the Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100) . Any Supplier that has participated in the process must provide documentation to confirm that they have completed the on-boarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS. This will accelerate the qualification process and at the same doesn't require the Supplier to demonstrate the compliance To initiate the on-boarding process, the Supplier should contact the CCCS Client Services to receive a copy of the onboarding	The Supplier must demonstrate how the Supplier of the proposed Commercially Available Software as a Service complies with the requirements in the Third Party Assurance Requirements. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments. The Supplier must provide each of the following industry certifications to demonstrate compliance: 1) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; and 2) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services; and 3) 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) Be valid as of the Submission date; b) Identify the legal business name of the proposed Commercially Available Software as a Service and Cloud Service Provider; c) Identify the current certification date and/or status; d) Identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report. e) The scope of the report must map to locations and services offered by the proposed Commercially Available Software as a 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; and

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		submission form and any additional information related to the CSP IT Assessment Program.	f) 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 system standard. The Supplier 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 assessment of its Services against the Cloud Security Alliance (CSA) Cloud Control's 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). Please note • Certifications must be provided for all portions of the proposed Service. • Certifications must be accompanied by assessment reports.
M9	**IT Security Assessment Program**	The Supplier must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services available (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) for the scope of the Services provided by the Supplier in the IT Security Assessment Program.	The Supplier must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services available (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) for the scope of the Services provided by the Supplier in the IT Security Assessment Program under Section 4 entitled “(Obligations Cloud Service Provider (CSP) IT Security Assessment Program)” of Annex B - Security & Privacy Obligations. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments. Mapping of the Security Controls must a included; GC Security Control Profile for Cloud-Based GC IT Services , and Industry Certification in Third-Party Assurance detailed under Tier 2 M8.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M10	**Supply Chain Management**	The Supplier 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 Software as a Service. For the purposes of this requirement, a company who is merely a supplier of goods to the Supplier of the proposed Commercially Available Software as a Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Software as a 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 Software as a Services of the Supplier has been proposed by the Supplier. Please note: Suppliers are advised that subsequent procurement Streams may require the Supplier to notify Canada regularly when there are updates to the list of third-party suppliers.	The Supplier 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 Software as a Service whether they would be (i) subcontractors to the Supplier, or (ii) subcontractors to subcontractors of the Supplier down the chain, OR (iii) any subsidiaries. The Supplier must fill out the Form 6 - SCI Submission Template as provided under this RFSA. If the Supplier does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Software as a Service, the Supplier is requested to indicate this in their response to this requirement. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M11	**Supply Chain Risk Management**	The Supplier of the proposed Commercially Available Software as a 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 Supplier must demonstrate how the Supplier of the proposed Commercially Available Software as a Service complies with the requirements in the Supply Chain Risk Management Requirements as documented under the Supplier Information Technology Security Assessment program. To be considered compliant, the provided documentation must demonstrate that the Commercially Available Software as a Service 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 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 Supplier’s approach to SCRM and demonstrate how the Suppliers of the proposed Commercially Available Software as a Service will reduce and mitigate supply chain risks. The SCRM Plan must be independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M12	**Privacy**	The Supplier of the proposed Commercially Available Software as a 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: Suppliers are advised that subsequent procurement Streams may require the Supplier to confirm to Canada on a regular basis that the proposed Commercially Available Software as a Service meets the above certification, and that the certification is valid for the full term of the procurement vehicle.	To demonstrate compliance to the certification, the Supplier must provide: a) A copy of the Commercially Available Software as a Service and Cloud Service Provider most recent and ISO 27018 certification documents, which must have been issued within 12 months prior to the Submission date; and b) A copy of the ISO 27018 assessment report for their current Commercially Available Software as a Services and Cloud Service Provider. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M13	**Privacy by Design**	The Supplier must demonstrate that it: (a) Implements a software development lifecycle that conforms to ISO 27032 and implements privacy by design; (b) Is compliant with the Privacy Management Framework and policy requirements that are specified in the ISO Standard 29100; and (c) (Adheres to the privacy by design 7 foundational principles (see https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M14	**Privileged Access Management**	The Supplier of the proposed Commercially Available Software as a Service must provide system documentation that demonstrates how to the Software as a service is able to meet the following security requirements Privileged Access Management Requirements: (a) Manage and monitor privileged access to the Solution, including the underlying infrastructure, to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services; (b) Restrict and minimize access to the Services and Canada's Information Assets to only authorized devices and End Users with an explicit need to have access; (c) Enforce and audit authorizations for access to the Services and Information Assets; (d) Constrain all access to service interfaces that host Assets and Information Assets to uniquely identified, authenticated and authorized End Users, devices, and processes (or services); (e) Implement password policies to protect credentials from compromise by either on-line or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials (ii) unusual use of credentials, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (f) Implement multi-factor authentication mechanisms to authenticate (Tier 2 only) End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (g) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Assets and Information Assets; (h) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles; (i) Adhere to the principles of least privilege and need-to-know when granting access to the Services and Assets and Information Assets;	The Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to meet the security requirements related to the Privileged Access Management Requirements: To be considered compliant, the provided documentation must include: a) System documentation or white paper that outlines the policies, processes and procedures used to manage privileged access management. The substantiation required for the Privileged Access Management , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		(j) Access controls on objects in storage and granular authorization policies to allow or limit access (k) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Services and Supplier Infrastructure; (l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and (m) Upon the termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.	

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M15	**Federation of Identity**	**Federation of Identity** The Supplier must have the ability for Canada to support federated identity integration including: (a) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Support for Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and (c) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding cloud service user account(s).	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Federation of Identity. 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 Federation of Identity. The substantiation required for in the Federation of Identity cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M16	**Endpoint Protection**	**Endpoint Protection** The Supplier must implement, manage, and monitor security-hardened endpoints to prevent against attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Endpoint Protection. 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 Endpoint Protection. The substantiation required for in the Endpoint Protection the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M17	**Secure Development**	**Secure Development** The Supplier must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Secure Development. 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 Secure Development. The substantiation required for in the Secure Development, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M18	**Supplier Remote Management**	**Supplier Remote Management** The Supplier must manage and monitor remote administration of the Supplier's Service that are used to host GC services and take reasonable measures to: (a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Employ a CSEC Approved Cryptographic Algorithmscryptographic mechanisms to protect the confidentiality of remote access sessions; (c) Route all remote access through controlled, monitored, and audited access control points; (d) Expeditiously disconnect or disable unauthorized remote management or remote access connections; (e) Authorize remote execution of privileged commands and remote access to security-relevant information.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Supplier Remote Management. 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 Supplier Remote Management The substantiation required for in the Supplier Remote Management, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M19	**Information Spillage**	**Information Spillage** (1) The Supplier must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, approved by Canada in writing. Notwithstanding the foregoing, the Supplier's Information Spillage process must include, at a minimum: (a) A process for identifying the specific data elements that is involved in a System's contamination; (b) A process to isolate and eradicate a contaminated System; and (c) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination. (d) The supplier will confirm a point of contact, proper procedures and an agreed upon secure form of communication to provide assistance where practicable for customer administrators. (2) Upon request of Canada, the Supplier must provide a document that describes the Supplier's Information Spillage Response Process. "Information Spillage (1) The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Submission; or (ii) another best practice of Leading Service Providers approved by Canada in writing. Notwithstanding the foregoing, the Supplier's Information Spillage process must include, at a minimum: (a) A process for identifying the specific Information Asset that is involved in an Asset's or System's contamination; (b) A process to isolate and eradicate a contaminated Asset or System; and (c) A process for identifying Assets or Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination. (2) The Supplier must provide an up-to-date information spillage process to Canada on an annual basis, or promptly following any Change to the Supplier's information spillage process.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Information Spillage. 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 Information Spillage. The substantiation required for in the Information Spillage, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M20	Cryptographic Protection	**Cryptographic Protection** The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Cryptographic Protection. (a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods; (b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111); (c) Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program), in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and (d) Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Cryptographic Protection 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 Cryptographic Protection The substantiation required for in the Cryptographic Protection, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.