Amendment 3 to the IaaS & Native PaaS Prequalification CBS

Solicitation No.	CS-IAAS-2024	Amd: 003

The purpose of this amendment is to:

1- Provide answers to questions received as detailed in section A.
2- Modify the Prequalification CBS as detailed in section B.

Section A - Questions and Answers (set 2)

Section	Question	Answer
SECTION 3 – Bid preparation instructions—prequalification	We would appreciate Canada's pre-bid review of the full Prequalification Bidding Form to ensure we are meeting or exceeding the Mandatory and Rated Criteria. Please confirm that Canada will conduct a pre-bid review on both Part A and Part B of the form.	No, as per paragraph a) and f) of section 3.2—Pre-Bid Compliance Check Process, Canada will review only Part A—Mandatory requirements of the Prequalification Bidding Form.
	For M2, if we submit the format we have of the current, latest version and valid industry certifications and audit reports (ISO/IEC 27001, ISO/IEC 27017, and SOC 2 Type II), will Canada confirm that the documents meet the criteria in advance to avoid confusion?	As part of the Pre-Bid Compliance Check Process, as detailed in paragraph e): If Canada does not note any deficiencies during its review of a Pre-Bid, Canada will provide the relevant Bidder with a "nil" response. The Bidder will still have to submit a bid and substantiation of its mandatory criteria at bid closing. The final determination of compliance for all Bidders is done after bid closing.
	Section 3.1 a) Will SSC accept multiple hyperlinks on the Prequalification Bidding Form wherever it asks for a "Publicly available hyperlink"?	SSC will accept only one hyperlink per cell on the Prequalification Bidding Form. Bidders should ensure that the provided hyperlink is the most relevant and direct link to the required information for the specific service in the category.
Prequalification Bidding Form	Will SSC accept a form signed electronically? (e.g., DocuSign)	The Prequalification Bidding Form (PBF), which is included as a separate attachment to the Prequalification CBS, contains a digital signature block that satisfies the signature and certification requirements. No additional signatures are required at this time.
	At the Stage 4 Bidder's Conference (on April 24, 2024, at 1:00 P.M. EDT), SSC indicated that if Bidders are including attachments/additional information along with their Prequalification Bidding Form response, that they should indicate this by clicking on a box under "Part B Rated—Prequalification Rated Criteria" within the form. There appears to be a few boxes to click. Does it matter which box Bidders click on?	When submitting additional documentation as a separate attachment alongside the Prequalification Bidding Form response, Bidders should check the box located under the specific requirement within "Part B Rated—Prequalification Rated Criteria" to which the documentation pertains. This will ensure that the relevant documentation can be easily searched for and found by Canada in relation to the relevant criteria.

	Section 2.3(a) states: "The Bidder may, as part of its Prequalification Bid, submit any additional cloud services terms not addressed by SECTION 6—RESULTING CONTRACT CLAUSES, including Annex A—Cloud General Terms and Conditions, for the Services being offered by the Bidder, i.e., terms that describe how cloud services are provisioned and how they may be ordered, deployed and used." Furthermore, paragraph (f) states: "Unless the additional cloud services terms proposed by the Bidder are included as a separate annex to the resulting contract, they will not be considered part of any resulting contract…". Can Canada confirm the following: The term bidder (small cap) in section 2 has the same meaning as the defined term in section 2.2b). If so, can Canada please make the correction? Since the resulting contract clauses are subject to further discussions in Stage 5, wave 4, Bidders can wait until then to submit their additional cloud service terms, or if they wish to submit at the prequalification stage, they will have the opportunity to update their additional terms in light of the final contract terms.	The term bidder (small cap) has the same meaning as the defined term in section 2.2b), Canada will make the correction. At this stage, the focus is on discussing and finalizing the contract clauses in Stage 5, wave 4. The resulting contract clauses are subject to further discussions and will be addressed in the next stage. Therefore, submitting additional cloud service terms is not required at this time.
	Can Canada please confirm the reason for the changes and the replacement of "person or entity… submitting a bid" with "originator of the public cloud service in its entirety" is only to prevent resellers from submitting a response and qualifying under this procurement process and is not intended to prevent the cloud service provider in any way from submitting a bid?	That is correct. The definition of Bidder is aligned with the obligations the Contractor will need to satisfy under the resulting contract. Only the originator will be able to satisfy the security requirement, so the definition is transparently changed to make it clear.
	Will the selected contract holders have the option to list authorized resellers? Or is SSC looking to transact directly with the cloud service providers only, and not include value-added resellers as part of the contract ecosystem?	For security reasons, only the originator of cloud services will be in position to satisfy the security obligations. Currently GoC don't have a security assessment process for resellers.
SECTION 5 — Certifications and additional information	In Section 5.1 The CBS states that certifications are no longer required for Prequalification and yet in 3.1 a) i) the Bid Document requires certifications. **Could you please confirm if any certifications are required and if so, specifically which certifications are required for Prequalification?**	For prequalification purposes, only the information outlined in the Prequalification Bidding Form is required. The reference in Section 3.1 a) to certifications pertains to the acceptance of the Rules of Engagement. Please note that paragraph 3.1 a) i) will be amended to reflect this clarification accurately.

		No specific certifications are required at the prequalification stage.
PART A — Mandatory Criteria	The prequalification criteria distinguish between “commercially available IaaS/PaaS services” and “unique services” (in R3). The way CSPs list their commercially available services may vary. For some CSPs, certain publicly listed services are best described as a “family” of various services vs. an individual service. For example, a publicly listed service may be a single entry in the list, but may have several different associated SKUs. Can Canada confirm that “commercially available cloud services” is intended to refer to the publicly listed cloud services/family of service, and that unique service refers to an individual service (with a specific SKU) regardless of whether it is listed on the publicly available list of services?	The definition of “unique services” applies only to R3. There is no term “unique services” in M1. M1 requires a single hyperlink per service that is within the CSP’s commercially available cloud services.
Part A— Mandatory Criteria M1	Mandatory Criteria 1. Example of what “instance types” means, can you give an example from a CSP so we can all align?	For the purpose of this solicitation, an instance type, in the context of cloud computing, refers to a virtual machine, serverless instance, or an add-on to a virtual machine offered by a cloud service provider.
Part A— Mandatory Criteria M1	Can Canada please clarify what is meant by a “service (instance type)”? We would typically assign each “instance type” a separate SKU. For example, for 1.b Compute optimized, we have instance types such as: X, Y, Z. These instance type names hint at a family within the service, a specialization and a size configuration. Based on the use of the word “instance type”, we would expect our product, such as “X”, to be one product.	Yes, this is correct. Please also **refer to the answer given above** for the definition of the Instance type.
Part A— Mandatory Criteria M1	Can Canada please clarify the use of the word processes in “iii. GPU-supported processes “ and provide examples? For example, do you mean processes like “ML Training” and “media encoding” or is it “processors”?	GPU-Supported Processes can include GPU Based Instances, adding GPU’s to other Instance Types, GPU’s for Machine Learning or Training are also acceptable. The intent of the 1d subcategories is to provide examples of what a Specialized Instances may be. Bidders are not required to provide a specific GPU example.
Part A— Mandatory Criteria M1 — Sub-requirement #1.F	The CBS requires us to provide 5 different IaaS Cold storage services for long-term archived data storage. Please clarify the intended purpose behind requesting five different archive storage options to ensure we accurately address your archiving needs. The industry best practice is to provide archive storage which is built upon object storage backbone, but with a lower access frequency. The general practice is to provide 1 or 2	Canada has revised M1 to adjust the minimum requirements for categories 5, 6, and 7 that should eliminate this concern without the need to combine 5 and 6.

	Archive storage service offerings which ultimately provide the best price-per-storage metric. Considering this, we request SSC to revise this requirement to be merged with Category 5 (e) for a total of 5 IaaS services requirement between categories 5 & 6.	
Part A—Mandatory Criteria M2	Mandatory Criteria 2. ISO 27001, ISO 27017/SOC2 for all the services or just the platform to be submitted with the response?	The third-party certification-requested focus on the maturity of the vendor in providing secure IT systems for cloud environments. **Prequalification stage**: For the purpose of substantiating compliance with M1, at Prequalification stage, Bidder must provide ISO 27001, ISO 27017 and SOC 2 Type II certifications that are given at the organization level. **Contracting Stage:** Prior contract award, the vendor will be required to identify which of their services are in-scope for ISO 27001, ISO 27017 and SOC 2 Type II certifications. The in-scope cloud services in detail will be assessed as per the CCCS Cloud service provider information technology security assessment process (ITSM.50.100). Services not covered by these third-party certifications cannot be assessed and cannot be included in the resulting contract.
Part A—Mandatory Criteria M2	Why does SSC require vendors to provide “a verification letter or statement from the issuing body (in a separate document)” when there is also a requirement to submit ISO/SOC2 certificates and audit reports? The certificates and audit reports themselves contain a signed certificate/preface from the issuing body with a signature from the reviewing official. We see the requirement to provide a letter or statement as redundant, and thus would request SSC to drop this documentation requirement.	The reason for this requirement (a verification letter or statement from the issuing body confirming the current and valid status of the certification) is to confirm the current and valid status of the certification. It is a relevant evidence and will not be changed.
Part B—Rated Criteria R1	The locations of our data centres are not public information. Would Canada reword the request to include the city, without precise physical address?	While Canada agreed to request only the city for Criterion R4, Criterion R1 will remain as currently stated, requiring the complete physical address to sufficiently demonstrate the evidence of the scoring element. As per the Prequalification Bidding Form, the form is protected B once submitted and is not available to the public.
Part B—Rated Criteria R2	This requirement seems to focus on rudimentary security capabilities to safeguard confidentiality. Would Canada consider additional measures to ascertain the capacity of the Bidder to enable Canada to secure its data? For example, the provider must/should have a cloud-native application protection platform	For this Prequalification, Canada is limiting the security questions to this requirement only. Prior to contract award, there will be stronger security obligations that the Bidder must meet.

	(CNAPP), which not only ensures continuous technical compliance but proactively supports the mitigation of threats and vulnerabilities.	
Part B—Rated Criteria R2 (1.B)	Requirements for data-in-transit and data-at-rest gives 1 point to “Encryption algorithm is on the list of CSE sufficient list.” However the referenced document (Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information—ITSP.40.111—Canadian Centre for Cyber Security) does not feature the list of “sufficient” crypto modules and algorithms. Where can the vendors find this list?	Canada has revised R2, which now references ITSP.40.062. This reference includes all the necessary for identifying the recommended and sufficient list. The changes to R2 include clarifications to both the scoring element and the evidence requirements.
Part B—Rated Criteria R2 (1.A)	This requirement provides maximum points for FIPS 140-3 CMVP validated modules. However there are hardly any CSPs with modules validated at this level (most of industry only has a FIPS 140-2 level validation). Request SSC to revise this requirement to allow maximum points for FIPS 140-2 level of validation. Alternatively, would SSC consider crypto modules which are under review FIPS review for the 140-3 level (i.e., validation in progress) for awarding the maximum points?	Canada has reviewed to R2 to allow for “undergoing review” for FIPS 140-3 level.
Part B—Rated Criteria R2 (1. A and 1.C)	In order to demonstrate our compliance, can the Bidder provide the reviewed list from NIST’s public site as evidence?	No, Bidders should not use the reviewed list from NIST’s public site as evidence to score points. Canada has reviewed R2, and both the scoring element and the evidence requirements have been clarified.
Part B—Rated Criteria R3	To demonstrate compliance, Bidders are required to provide information about clients that is commercially confidential. Of main concern is the list of services—identifying what services a customer is using is not something we can disclose. Without authorization from the client to disclose this information, Bidder would be unable to substantiate compliance based on the current drafting of the requirement. There are different ways to assess this capability without requesting this level of granularity. Will an aggregated number of services that a client runs be acceptable?	As per R3, information to be provided by Bidders, an aggregated number of unique services provided and used by the client within the duration of services is fully acceptable.
Part B—Rated Criteria R3	As it relates to the duration, we question the need for seven (7) or more years for customer references. This industry has changed so rapidly that services available seven or more years ago in many cases have significantly changed or evolved. What is the government trying to accomplish with awarding additional points for a 7+ years duration? None of the metrics outlined in	Canada is assessing the experience of the Bidder to provide IaaS and native PaaS Services to large organizations. The duration of the services is a valuable metric to compare experience.

	the I-CBS document (duration/services/# of employees) measure technical or business capabilities—how do you define a “service”?	As per R3, in this criterion “unique services” means a specific element of the commercially and publicly available cloud services catalog. This specifically excludes non-public cloud services such as private cloud services and data centre hosting services.
Part B—Rated Criteria R4	Many services offered are actually “serverless” and not Core based, in which case it does not make sense to measure the capacity all the services from CSP	Serverless computing does utilize compute resources. Serverless computing is a cloud computing model whereby the cloud provider dynamically manages and allocates CPU cores for executing code without requiring the consumer to provision or manage resources explicitly. Canada’s objective for this element is to determine how many cores the provider has to offer across all services including serverless solutions.
Part B—Rated Criteria R4	This rated requirement appears to focus on the GC’s legacy model and doesn’t align with the innovative approach or concept of the CBS (Canada presents the requirement as a need [problem statement(s)] and allows industry the freedom to propose innovative solutions that fill the need). This requirement doesn’t have a business outcome or objective. For example, what business outcome requires the need to know how many CPU cores are deployed in Canada?	Canada has determined that R4 provides a point in time view of the Bidder’s capacity to address Canada’s needs. In subsequent stages of the procurement process, the prequalified Bidders will be invited to provide suggestions on how best to resolve Canada’s problems and challenges.
Part B—Rated Criteria R4	Will Canada please clarify if the definition of a Data Centre should include edge locations, co-location sites and points of presence or simply the data centres hosting the zones within a region?	Canada has reviewed the definition and provided an additional definition of Data Centre in R1.
Part B—Rated Criteria R4	There are different ways to calculate network capacity. Will Canada please clarify if it is the capacity of peering through point of presence and edge? Or, is it the capacity of the internal link between regions or zones? Please provide an example of a suitable calculation.	Canada has revised R4 to clarify the terminology and has included a requirement for a daily average from February 1 to February 29, 2024, to establish a fixed time frame.
Part B—Rated Criteria R4—Sub-requirement #5	What does “Number of network connections in Canada” exactly mean? Does it refer to the ‘network service provider partners’ that the vendor partners with to be able connect GC EDCs to CSP networks in a private/dedicated fashion?	

Part B—Rated Criteria 4, element 7	What does “Bandwidth capacity” in gigabits per second in Canada actually refer to? Bandwidth capacity of what component exactly? Similarly, in R4, what does “Number of network connections in Canada” refer to exactly? Are we referring to 3rd party partner companies who can provide connectivity between GC EDCs and the CSP DC?	
Part B—Rated Criteria R4—Sub-requirement #7	Regarding “Bandwidth capacity in gigabits per second in Canada.” — Could SSC clarify what bandwidth capacity is being referring to? Does this refer to the total port speed capacity available with CSP to enable dedicated/private connectivity to on-prem networks?	
Part B—Rated Criteria R4—Sub-requirement #8	We request SSC to provide more clarity & definition around the exact requirement as pertains to” Total number of cores deployed in Canada.”	
Part B—Rated Criteria R4—elements 8 and 9	“Total number of cores deployed in Canada”.. are you referring to 'Cores' of just the IaaS Compute services? or the capacity of EVERY IaaS/PaaS/SaaS service that CSP offers?	Canada’s objective for this element is to determine how many cores the provider has to offer across all services included in IaaS and Native PaaS solutions within Canada. As long as the Bidder is able to allocate or reallocate the considered cores to IaaS\Native PaaS for leverage in the solution, then these cores can be considered for the calculation.
Part B—Rated Criteria R4	How would SSC allocate points when there are one or more ties in the ranking order for a particular sub-requirement? For example, for the number of regions in Canada — many CSPs have two regions which results in a tie among many vendors.	In the event of a tie in the ranking order for a particular element, all Bidders with the same ranking will receive the same score. For example, with eight Bidders: if two Bidders have five regions, they will receive the highest score of three points each. If two Bidders have three regions, they will both rank second and receive two points each. Finally, if three Bidders have one region, each Bidder will be ranked third rank and will receive one point.
General — procurement process	Does SSC expect to receive input on the terms and conditions that are unrelated to security and privacy?	The terms and conditions will be discussed with prequalified Bidders in ITR wave 4.

Section B — Modifications to the Solicitation

1- In the solicitation, Section 2.3(f)

Delete: Unless the additional cloud services terms proposed by the **bidder** are included as a separate annex to the resulting contract, they will not be considered part of any resulting contract (even if they are part of the bid that is incorporated by reference into the resulting contract). The fact that some additional terms and conditions were included in the bid will not result in those terms applying to any resulting contract, regardless of whether or not Canada has objected to them under the procedures described above.

Replace with: Unless the additional cloud services terms proposed by the **Bidder** are included as a separate annex to the resulting contract, they will not be considered part of any resulting contract (even if they are part of the bid that is incorporated by reference into the resulting contract). The fact that some additional terms and conditions were included in the bid will not result in those terms applying to any resulting contract, regardless of whether or not Canada has objected to them under the procedures described above.

2- In Attachment 1—Prequalification Evaluation Grid, Part A—Mandatory Criteria

Canada has modified M1, R1, R2 and R4

Delete: the Prequalification Evaluation Grid, in its entirety
Replace with the updated Attachment 1 — Amd001

3- In the Prequalification Documents

Delete: Bid Document 1—Prequalification Bidding Form, in its entirety

Note: the new version of the Prequalification Bidding Form will be provided shortly.

We have received a lot of feedback, and priority is being given to comments related to the current prequalification phase. All other aspects, such as terms and conditions, resulting contracts, task allocation process, will be addressed, with the prequalified vendors, in the upcoming stages.

All other terms and conditions remain unchanged.

Prequalification

Part A — Mandatory Criteria

The following mandatory criteria must be met.

	Criteria	Information required by Bidders	Scoring Elements
M1	**Capacity of the Bidder to sell Commercially Available Infrastructure-as-a-Service (IaaS) AND Platform-as-a-Service (PaaS)** The Bidder must be a Cloud Service Provider (CSP) with Commercially Available Infrastructure-as-a-Service (IaaS) services **AND** Native Platform-as-a-Service (PaaS) services. For the purpose of this criterion, an instance type, in the context of cloud computing, refers to a virtual machine, serverless instance, or an add-on to a virtual machine offered by a cloud service provider.	The Bidder should provide the hyperlink publicly available listing the Commercially Available IaaS and Native PaaS services of the following: 1. services (instance types) that address each category of the following Commercially Available IaaS services: a. Category 1—General or Standard Purpose instances that are configurable to balance the amount of compute, memory, and networking resources based on the requirements of applications and workloads. b. Category 2—Compute Optimized instances for applications and workloads that require high computing power using high-performance processors. c. Category 3—Memory Optimized instances for applications and workloads that require fast processing of large data sets in memory. d. Category 4—Specialized instances for applications and workloads that require specific requirements, including any of the following sub-categories: i. High-Performance Computing (HPC) ii. Enhanced storage capabilities iii. GPU-supported processes iv. Machine learning-based systems e. Category 5—Block, Object and File storage capabilities that are scalable. f. Category 6—Cold storage for long-term storage of archived data. g. Category 7—High-Performance storage based on Solid-State Drives (SSD) technology. 2. services (instances type) that address each category of the following Native PaaS services: a. Category 8—Container services b. Category 9—Developer tools c. Category 10—Database services d. Category 11—Network and security services e. Category 12—Artificial Intelligence (AI) or Machine Learning (ML) f. Category 13—Analytics and Big Data services	To be compliant, the Bidder must demonstrate the following services through hyperlinks: • A minimum of 5 Commercially Available IaaS services for each of the categories 1 to 4 evidenced by their publicly viewable product/service list (1a to 1d) • A minimum of 3 Commercially Available IaaS services for category 5 evidenced by their publicly viewable product/service list (1e) • A minimum of 1 Commercially Available IaaS service for each of the categories 6 and 7 evidenced by their publicly viewable product/service list (1f and 1g) • A minimum of 4 Commercially Available PaaS services for each of the categories 8 to 13 evidenced by their publicly viewable product/service list (2a to 2f) The Bidder should provide a hyperlink that allows Canada to easily access to the relevant evidence. Canada may, but have no obligation, contact the Bidder to arrange a meeting to facilitate a session where the Bidder will show Canada where the information is within hyperlink that was provided at bid closing. Information located in hyperlink other than the one provided as part of the bid will not be considered.

	Criteria	Information required by Bidders	Scoring Elements
M2	**Capacity of the Bidder to secure Canada’s Data** The Bidder must have the following current, latest version and valid industry certifications and audit reports: 1. ISO/IEC 27001: Information technology — Security techniques—Information security management systems — Requirements; 2. ISO/IEC 27017: Information technology — Security techniques—Code of practice for information security controls based on ISO/IEC 27002: for cloud services; 3. AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality. *Only certifications issued by an independent third party qualified under AICPA, CPA Canada, or conforming to the ISO/IEC 17020 quality system standard will be accepted.	The Bidder should provide the following evidence for each certification and audit reports: - copies of the certifications and audit reports. - a verification letter or statement from the issuing body confirming the current and valid status of the certification. - the date of issuance and expiration (as applicable).	To be compliant, the Bidder must demonstrate they have current, latest version and valid certifications and audit reports of the following: ISO/IEC 27001, ISO/IEC 27017 and AICPA Service Organization Control (SOC) 2 Type II.

Part B — Rated Criteria

The following criteria will be rated as per the scoring elements defined in the table.

Maximum total score = 77 points

	Criteria	Information to be provided by Bidders	Scoring Elements
R1	**Capacity to satisfy data residency requirements (maximum 15 points)** The Bidder should have a minimum of two data centres located in a single region in Canada. Canada uses the Uptime Institute’s Tiered Classification System for the Data Centre definition. For the purpose of this solicitation: A Data Centre (DC) is a physical infrastructure that meets or exceeds the “Data Centre Tier III” requirements. A DC is part of a region. A region is defined as multiple DC’s located within 100 km of each other within the same defined region.	The Bidder should provide the physical address of two data centres located in a single region in Canada.	Up to 15 points will be allocated. Points will be allocated as follows: **15 points:** the Bidder has provided the physical address of 2 data centres located in a single region in Canada. **10 points:** the Bidder has provided the physical address of 2 data centres located in Canada not within the same region. **5 points:** the Bidder has provided the physical address of one data centre located in Canada. **0 points:** the Bidder has not provided the physical address of any data centre located in Canada.
R2	**Capacity of the Bidder’s Solution to protect Canada’s data (maximum 12 points)** The Bidder should demonstrate that the Solution has the capability to encrypt data-in-transit and data-at-rest with Communications Security Establishment Canada (CSE) approved cryptography. The CSE approved cryptography can be found in the Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information—ITSP.40.111 (version 3 — March 18, 2024) (https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111) and Guidance on securely configuring network protocols (ITSP.40.062) (revision 2—August 21, 2020) (www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062) *Note to Bidders: This requirement is not mandatory for the prequalification stage. In subsequent procurement stages, we will require all cryptographic mechanisms and subsequent modules and algorithms used and they will be verified prior to contract award.*	**1. For Data-in-transit:** To demonstrate its capacity, the Bidder should provide one cryptographic mechanism used to prevent unauthorized disclosure of information and detect changes to information during transmission, and provide evidence for the following elements: a) Identify if the Cryptographic module has been tested and validated or is undergoing review under the Cryptographic Module Validation Program (CMVP) for compliance to FIPS 140-3: Security Requirements for Cryptographic Module as per Section 12 of ITSP 40.111 For validated module: Bidder should provide the module name and the certificate number. For module undergoing review: Bidder should provide a confirmation from the Lab that the module is at or passed “Step 3—in review” for FIPS 140-3 validation. b) Identify one implemented encryption algorithm that satisfies section 2 and 3 of ITSP 40.111 and is on one of the tables (Tables 1 to 21) of ITSP.40.062. Bidders should provide the algorithm name and the applicable table in the ITSP.40.062. c) Confirm whether Cryptographic algorithm	Up to 12 points will be allocated. **1. For Data-in-transit:** Points will be allocated as follows: a) Cryptographic module: **2 points:** The Bidder has provided a certificate number demonstrating that the module is FIPS 140-3 validated by the CMVP or has provided a confirmation from the Lab that the module is at or passed “Step 3—in review” for FIPS 140-3 validation by the CMVP. **1 point:** The Bidder has provided a certificate number demonstrating that the module is validated under a previous version of FIPS 140-3 by the CMVP. **0 points**: Not CMVP validated. b) Encryption algorithm: **2 points:** The encryption algorithm implemented is on one of the tables (Tables 1 to 21) under the recommended column in the ITSP.40.062. **1 point:** The encryption algorithm implemented is on one of the tables (Tables 1 to 21) under the sufficient column in the ITSP.40.062.

	Criteria	Information to be provided by Bidders	Scoring Elements
		implementations have been tested and validated under the Cryptographic Algorithm Validation Program (CAVP) as per Section 12 of ITSP 40.111. Bidders should provide the validation number **2. For Data-at-rest:** To demonstrate its capacity, the Bidder should provide one cryptographic mechanism used to prevent unauthorized disclosure and modification of the information at rest on information system components storing Canada's data and provide evidence for the following elements: a) Identify if the Cryptographic modules have been tested and validated or are undergoing review under the Cryptographic Module Validation Program (CMVP) for compliance to FIPS 140-3: Security Requirements for Cryptographic Modules as per Section 12 of ITSP 40.111 For validated modules: Bidder should provide the module name and the certificate number. For module undergoing review: Bidder should provide a confirmation from the Lab that the module is at or passed "Step 3—in review" for FIPS 140-3 validation. b) Identify one implemented encryption algorithm that satisfies section 2 and 3 of ITSP 40.111 and is on one of the tables (Tables 1 to 21) of ITSP.40.062. Bidders should provide the algorithm name and the applicable table in the ITSP.40.062. c) Confirm whether Cryptographic algorithm implementations have been tested and validated under the Cryptographic Algorithm Validation Program (CAVP) as per Section 12 of ITSP 40.111. Bidders should provide the validation number.	**0 points:** Any other algorithm not in one of the tables under recommended and sufficient columns in the ITSP.40. c) Cryptographic algorithm: **2 points:** The Bidder has provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP **0 points:** The Bidder has not provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP **2. For Data-at-rest:** Points will be allocated as follows: a) Cryptographic module: **2 points:** The Bidder has provided a certificate number demonstrating that the module is FIPS 140-3 validated by the CMVP or has provided a confirmation from the Lab that the module is at or passed "Step 3—in review" for FIPS 140-3 validation by the CMVP. **1 point:** The Bidder has provided a certificate number demonstrating that the module is validated under a previous version of FIPS 140-3 by the CMVP. **0 points:** Not CMVP validated. b) Encryption algorithm: **2 points:** The encryption algorithm implemented is on one of the tables (Tables 1 to 21) under the recommended column in the ITSP.40.062. **1 point:** The encryption algorithm implemented is on one of the tables (Tables 1 to 21) under the sufficient column in the ITSP.40.062. **0 points:** Any other algorithm not in one of the tables under recommended and sufficient columns in the ITSP.40. c) Cryptographic algorithm: **2 points:** The Bidder has provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP. **0 points:** The Bidder has not provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP.
R3	**Experience of the Bidder to provide IaaS and Native PaaS services to large organizations (maximum 21 points)**	To demonstrate its experience, the Bidder should provide a list of three clients to whom both IaaS and Native PaaS services were provided.	Up to 21 points will be allocated using the average of the three clients' total points. Points will be allocated as follows:

	Criteria	Information to be provided by Bidders	Scoring Elements
	The Bidder should demonstrate its experience in providing both IaaS and Native PaaS services to large government organizations or large external private corporations. *“external” refers to organizations or corporations that are not part of the Bidder’s own corporate structure or its parent organization.* For the purpose of this criterion “unique services” means a specific element of the commercially and publicly available cloud services catalog. This specifically excludes non-public cloud services such as private cloud services and data centre hosting services.	For each client, the following information should be provided: 1) Client business name 2) Duration of services including service start date and end date (if applicable) (month and year) 3) Number of employees of the client 4) Number of unique services provided and used by the client within the duration of services.	**Duration of services rendered to the client** **7 points:** more than or equal to 7 years **5 points:** more than or equal to 5 years and less than 7 years **3 points:** more than or equal to 3 years and less than 5 years **0 points:** less than 3 years **Number of employees of the client** **7 points:** 50,000 employees and more **5 points:** between 29,999 and 50,000 employees **3 points:** between 9,999 and 30,000 employees **0 points:** fewer than 10,000 employees **Unique services provided and used** **7 points:** 200 services and more **5 points:** between 149 and 200 services **3 points:** between 99 and 150 services **0 points:** fewer than 100 services If more than three clients are submitted, only the first three clients listed in the submission will be assessed.
R4	**Capacity of the Bidder to address Canada’s needs (maximum of 29 points)** The Bidder should demonstrate its capacity to address Canada’s needs	The Bidder should provide the following information to demonstrate its capacity to address Canada’s needs for each element listed below: **Elements of comparison** 1. Number of Regions in Canada. 2. Number of Regions in the World. 3. Number of Data Centres (DC) in Canada. The Bidder should provide the city of each DC associated with the region. 4. Total number of Data Centres deployed and in service in the World. 5. Number of internet exchange points in Canada. The Bidder should provide the name of the corporations of each internet exchange point providers they are with. 6. Number of internet exchange points globally. 7. Internet bandwidth capacity in gigabits per second in Canada. The Bidder should provide the gigabits per second. 8. Daily average number of cores deployed in Canada from February 1, 2024 to February 29, 2024.	Up to 29 points will be allocated using the sum of the comparative assessment and direct scoring of the elements (1 to 11). Each element (1 to 11) will individually be assigned points. **Comparative assessment of elements** For elements 1 to 9: A. **Establishing the ranking**: Bidder will be ranked from the highest number to the lowest number. B. **Allocating the points:** points will be allocated based on the Bidder’s ranking in each element, from highest to the lowest. Points will be allocated for each element of comparison as follows: **3 points:** Top rank Bidder **2 points:** Second rank Bidder **1 point:** Third rank Bidder **0 points:** Remaining ranked Bidder (4+) In the event of a tie in the ranking order for a particular element of comparison, all Bidders with equal rankings will receive the same score.

	Criteria	Information to be provided by Bidders	Scoring Elements
		9. Percentage of available capacity in terms of cores. The Bidder should provide the data associated with the following calculation: The percentage of available capacity in terms of cores is calculated by [1-daily average number of cores in use in Canada from February 1, 2024 to February 29, 2024/by the daily average number of cores deployed in Canada from February 1, 2024 to February 29, 2024 (item 8)]*100. **Direct scoring** 10. The Bidder has documentation that defines latency and performance metrics between their Canadian regions: yes or no 11. The Bidder offers a Marketplace for 3rd party apps: yes or no For elements 10 and 11: The Bidder should provide the hyperlinks.	**Direct scoring of the elements** For elements 10 and 11, points will be allocated as follows: **1 point:** Yes **0 points:** No