Correctional Service Canada Service correctionnel Canada

RETURN RESPONSES TO :
RETOURNER LES RÉPONSES À :
Receiving Office - Bureau de réception:

bidsubmissions.GEN-NHQContracting@CSC-SCC.GC.CA

REQUEST FOR INFORMATION
DEMANDE DE RENSEIGNEMENTS

Comments — Commentaires :

Vendor/Firm Name and Address —
Raison sociale et adresse du fournisseur/de l'entrepreneur :

____

____

____

____

Telephone # — Nº de Téléphone :
____

Fax # — No de télécopieur :
____

Email / Courriel : ________________________

GST # or SIN or Business # — Nº de TPS
ou NAS ou Nº d'entreprise :
____

Title — Sujet : OMS Data Foundation	
Request for information (RFI) No. — Nº. de la demande de renseignements (DDR) : 21120-20-3246369	**Date :** July 15, 2019
Client Reference No. — Nº. de Référence du Client 21120-20-3246369	
GETS Reference No. — Nº. de Référence de SEAG 21120-20-3246369	
RFI Closes — La DDR prend fin **at /à :** 2:00 DST **on / le :** August 28, 2019	
F.O.B. — F.A.B. Plant – Usine: Destination: Other-Autre:	
Address Enquiries to — Soumettre toutes questions à: Steve Perron Steve.perron@csc-scc.gc.ca	
Telephone No. – Nº de téléphone: 613-992-6509	**Fax No. – Nº de télécopieur:**
Destination of Goods, Services and Construction: **Destination des biens, services et construction:**	
Instructions: See Herein **Instructions : Voir aux présentes**	
Delivery Required — Livraison exigée : See herein	**Delivery Offered – Livrasion proposée :** Voir aux présentes
Name and title of person authorized to sign on behalf of Vendor/Firm **Nom et titre du signataire autorisé du fournisseur/de l'entrepreneur** _______________________________________ Name / Nom Title / Titre _______________________________________ Signature Date	

Table of Contents

1.0 Background

1.1 Correctional Service of Canada

The Correctional Service of Canada (CSC) is a Government of Canada (GC) agency within the portfolio of Public Safety Canada https://www.publicsafety.gc.ca/. Public Safety Canada works with five agencies and three review bodies, united in a single portfolio and all reporting to the Minister of Public Safety.

CSC helps protect society by encouraging offenders to become law-abiding citizens while exercising reasonable, safe, secure and humane control. CSC is responsible for managing offenders sentenced to two years or more in federal correctional institutions and under community supervision. CSC is currently responsible for approximately 15,500 offenders incarcerated in institutions and 8,700 offenders under supervision in the community.

CSC has a presence from coast to coast, from large urban centres with increasingly diverse populations, to more remote communities across the North. CSC manages institutions, psychiatric treatment centres, four Aboriginal healing lodges, community correctional centres, community residential facilities and parole offices. In addition, CSC has six regional headquarters that provide management and administrative support and serve as the delivery arm of CSC’s programs and services.

1.1.1 The Offender Management System (OMS)

The Offender Management System (OMS) is CSC’s current mission critical application, used to manage offenders under its care and ensure their reintegration into society while ensuring the safety of Canadians. Besides being utilized directly by its partner, the Parole Board of Canada, CSC also uses OMS to share offender information electronically with other stakeholders such as the Canadian Police Information Centre (CPIC), Passport Canada, InfoPol, the Canada Revenue Agency and Provincial Governments.

The current version of OMS was implemented by CSC in 2003 and uses a Windows-based distributed application with an Oracle database. Offender data is segregated by region across five data centres and then replicated to central databases for consolidation, interface processing, extracts to ancillary internal and external systems, the data warehouse and for business continuity.

Shifts to cloud based computing, service-oriented architecture and application programming interfaces, open source, mobile devices and predictive analytics are hampered by the nature of the OMS legacy architecture.

As of June 2017, OMS had approximately 15,000 active user accounts which included 14,000 CSC internal and 1,000 external users. There are approximately 500-600 concurrent users at peak times, geographically disbursed across the country. The application holds information for approximately 100,000 inactive and current offenders.

1.1.2 OMS Data Foundation Project

The OMS Data Foundation project is a multi-year endeavour that was initiated in 2017. The goals of the project are to improve offender data quality, consistency and governance, and establish an information landscape that enables the exchange of the right information to the right people at the right time, is built on a modern, cloud-ready architecture, and can more quickly implement new or changing business policies and legislation.

The capabilities introduced by the project will also enable CSC to take advantage of new technologies, tools and techniques for capturing, managing and analyzing offender data.

From an overall perspective, the Data Foundation project aims:

- To improve data quality and access resulting in better, more consistent decision making to benefit both offenders and public safety;
- To modernize the data architecture, toolset, and deploy a reusable set of services to become more agile, scalable and improve time to market in responding to changing legislation, business policy or advances in technology;
- To improve data sharing and interoperability with criminal justice partners;
- To define key data governance practices, roles and responsibilities, processes, policies and standards; and
- To comply with Government of Canada standards and directives, such as:
    - https://www.canada.ca/en/government/publicservice/modernizing/government-canada-digital-standards.html
    - https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249
    - https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-cloud-adoption-strategy.html
    - https://open.canada.ca/en

For the purposes of this RFI, the focus is on the modernization of the data architecture and landscape; most specifically, the database.

1.1.3 Modernization of the Data Architecture and Landscape

The current offender data landscape involves data segregation across five regional data centres with replication and consolidation to a central National Headquarters (NHQ) database. The offender data is stored in a relational data model that has expanded over the past 20 years as the application has evolved to meet new legislative, business or policy requirements.

All of the offender applications and data components are currently hosted in regional or NHQ data centres. The future vision is to move to a data service-based architecture, allowing CSC to begin the migration of application components to the cloud to align with Government of Canada standards and directives.

The Data Foundation project will establish the architecture, procedures and transition plan for this migration to the cloud and includes the following high-level goals:

- ➢ Establish a cloud-based API architecture and technology components on which to build the next generation of offender management capabilities
- ➢ Establish a CSC Protected B cloud environment for hosting the data services
- ➢ Establish the procedures and transition plan for offender data migration to the cloud
  - o Establish a new data platform in CSC's Protected B cloud environment and begin to build the new offender data model
  - o Establish the architecture, tools, procedures and transition plan to migrate offender data to the new cloud data platform and to synchronize the new data elements in the cloud with the on-premise legacy databases.

*Note: Protected B refers to a specific Security level for sensitive government information and assets. Please refer to https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html for more information.

1.1.4 Solution Approach

Based upon Government of Canada standards and directives, project research and a recent in-house proof of concept, the Data Foundation project has selected an end-to-end JavaScript technology stack (Angular, Node and Express) and is now considering the available options for an enterprise cloud-based, object-oriented data model.

The project will implement a national database in the CSC Protected B cloud environment using either Software as a Service (SaaS) or Infrastructure as a Service (IaaS) to host the database. At the time of this RFI, SaaS is the preferred approach. There is also a preference to leverage an Open Source solution.

Migration of existing offender data to the new enterprise database will be done incrementally as new business web applications and APIs are developed and deployed. Data Foundation will establish the processes, procedures and transition plan to move offender data to the new cloud-based data platform. This will enable future business initiatives to migrate data from the legacy database over time.

The database solution selected must be able to operate seamlessly in a hybrid landscape that includes cloud and legacy applications and data.

1.2 Objectives of this Request for Information

The purpose of this Request for Information (RFI) is for the Information Management Services (IMS) division of CSC to gather information on industry capabilities for cloud-based, object-oriented database management systems (known henceforth in this document as the "Database") that will support CSC's modern architecture.

Respondents should provide feedback on database options, their capabilities and best fit in a Protected B cloud environment supporting a hybrid landscape of offender data and related business applications.

CSC is open to considering a wide range of database solution options. In addition to Respondents that offer their own database product, CSC encourages system integrators and other technology suppliers that partner with database providers to consider this RFI. Also, Respondents that support a variety of database offerings are encouraged to respond with more than one option.

2.0 The RFI Process

2.1 Nature of the RFI

This request for information is neither a call for tender or a Request for Proposal. No agreement or contract will be entered into based on this RFI. The issuance of this RFI is not to be considered in any way as a commitment by the Government of Canada, nor as authority to potential respondents to undertake any work that could be charged to Canada. Potential suppliers of any goods or services described in this RFI should not reserve stock or facilities, nor allocate resources, as a result of any information contained in this RFI. Nor will this RFI result in the creation of any source lists.

This RFI is not to be considered as a commitment by the governments of Canada to issue a subsequent solicitation or award contract(s) for the work described herein. This RFI is simply intended to solicit feedback from industry with respect to the subject matter described in this RFI.

Although the information collected may be provided as commercial-in-confidence (and, if identified as such will be treated accordingly by Canada), Canada may use the information to assist in drafting performance specifications (which are subject to change) and for budgetary purposes.

Respondents are encouraged to identify, in the information they share with Canada, any information that they feel is proprietary, third-party or personal information. Please note that Canada may be obligated by law (e.g. in response to a request under the Access to Information and Privacy Act) to disclose proprietary or commercially-sensitive information concerning a respondent (for more information: http://laws-lois.justice.gc.ca/eng/acts/a-1/).

Participation in this RFI is encouraged, but not mandatory. There will be no short-listing of potential suppliers for the purposes of undertaking any future work as a result of this RFI. Similarly, participation in this RFI is not a condition or prerequisite for the participation in any potential subsequent solicitation.

2.2 Nature and Format of Responses Requested

Respondents are requested to review *Annex A - Response Requirements* and prepare responses following the structure outlined therein.

Respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this RFI could be satisfied. Respondents should review *Annex B – CSC Technical Environment Information* and explain any assumptions made in preparation of their responses.

Responses from Respondents will assist CSC in formulating a procurement strategy that meets the business and operational requirements of CSC.

Respondents are free to submit information on other software, which are related to the proposed Database, or work in conjunction with the proposed Database, to support data synchronization, data migration or any other functionality that the Respondent may deem applicable.

2.3 Response Parameters

Respondents may submit comments, concerns, suggestions, and, where applicable, alternative recommendations regarding how the requirement may be satisfied.

2.4 Response Confidentiality

Respondents are requested to clearly identify those portions of their response that are proprietary to the Respondent. Canada will handle the responses in accordance with the Access to Information Act.

2.5 Response Costs

Canada will not reimburse any organization for expenses incurred in responding to this RFI. Participants are responsible for their own transportation, accommodation, meals, parking and all other expenses related to engagement activities. Canada will not reimburse any supplier or participants for expenses incurred in responding to Canada's questions or attending any meetings or other events during the engagement process.

2.6 Treatment of Responses

2.6.1 Use of Responses

Responses received by the RFI closing date will not be formally evaluated. They will be reviewed and may be used by CSC to develop or modify procurement strategies or any draft documents contained in this RFI. CSC may, at its discretion, review responses received before or after the RFI closing date.

2.6.2 Review Team

A review team composed of representatives of the Correctional service of Canada (CSC) will review the responses. Canada reserves the right to hire any additional independent consultants, or use any Government of Canada (GC) resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

2.6.3 Confidentiality

Respondents should mark any portions of their response that they consider proprietary or confidential. CSC will handle the responses in accordance with the *Access to Information Act*.

2.6.4 Follow-up Activity

CSC may, at its sole discretion, contact any respondents to follow-up with additional questions or for clarification of any aspect of a response. CSC reserves the right to invite any or all respondents to present their submissions to this RFI and/or perform a product demonstration (herein referred to as a “Respondent Session”).

Respondents that have expressed such interest can expect to be contacted within approximately four (4) weeks after the RFI closing date to schedule the Respondent Session. An Invite Agenda along with specific questions or areas of interest to be covered during the session will be provided to the invited respondents.

The Respondent Session will be located in the National Capital Region (NCR). The exact location and timeframe will be detailed in the Invite Agenda. Respondents will also be asked to provide an electronic version of their presentation.

The Respondent Session will cover specific functional and technical aspects of the Solution. As such, Respondent representatives attending the session must include Subject Matter Expert(s) in these areas in order to meaningfully respond to questions at the session. CSC personnel with extensive experience in IT technology will attend the presentation.

2.7 Response Format

2.7.1 Response Preparation Instructions

CSC requests that the Respondent provide their responses in separately bound sections as follows:

a. One hard copy and one soft copy on CD in a Microsoft Word Format. CSC requests that Respondents follow the instructions described below in the preparation of their response:

    i. use 8.5 x 11 inch (216 mm x 279 mm) paper; and
    ii. use a numbering system that corresponds to the RFI.

b. In accordance with the *Policy on Green Procurement*. In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process *Policy on Green Procurement* (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, Respondents should:

i. use 8.5 x 11 inch (216 mm x 279 mm) paper containing fibre certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and

ii. use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

c. Respondents are reminded that this is an RFI and not a Request for Proposal (RFP) and, in that regard, respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this RFI could be satisfied.

i. RFI responses should clearly identify any additional information and/or clarification that respondents suggest be incorporated into any future solicitation documents. Respondents are also invited to provide comments regarding the content, format and/or organization of any draft documents included in this RFI.

ii. Respondents should explain any assumptions they make in their responses. Any marketing or promotional information submitted as part of the responses will not be reviewed.

iii. Responses will not be used for competitive or comparative evaluation purposes. Respondents should feel free to submit whatever information they feel would make a useful and relevant contribution to the development of solicitation documents to procure the goods and/or services to meet CSC’s requirements.

d. For ease-of-use and in order that the greatest value be gained from responses, CSC requests that any submissions to this RFI cite the questions appearing in Annex A to which the respondents’ information pertains. This will assist CSC in gathering and collating submission information addressing specific areas of the requirement.

e. Changes to this RFI may occur and will be advertised on the Government Electronic Tendering System. Canada asks respondents to visit Buyandsell.GC.ca regularly to check for changes, if any.

f. The information contained in this document remains a work in progress and respondents should assume that CSC may add new requirements to any solicitation that is ultimately published by Canada, and respondents should assume that CSC may delete or revise some of the requirements, at its own discretion.

2.7.2 Volume Cover Page

If the response includes multiple volumes, respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number, the total number of volumes and the full legal name of the respondent.

2.7.3 Title Page

The first page of each volume of the response, after the volume cover page, should be the title page, which should contain the:

- Title of the respondent's response;
- Volume number and the total number of volumes;
- Name and address of the respondent;
- Name, address and telephone number of the respondent's contact;
- Date; and
- RFI number.

2.7.4 Numbering System

Respondents are requested to prepare their response using a numbering system corresponding to the one used in this RFI. All references to descriptive material, technical manuals and brochures included, as part of the response, should be referenced accordingly.

2.7.5 Language of Response

Responses may be in English or French at the preference of the Respondent.

2.8 Enquiries

As this is not a bid solicitation, CSC will not necessarily respond to enquiries in writing or by circulating answers to all potential suppliers. However, respondents with questions regarding this RFI may direct their enquiries to:

Contracting Authority:

Steve Perron
Senior Procurement Officer – Contracting Operations
National Headquarters
Correctional Service Canada
T. 613-992-6509
E. steve.perron@csc-scc.gc.ca

2.9 Submission of Responses

Respondents interested in providing a response **must** deliver it to the Contracting Authority identified above by **14:00 DST on August 28, 2019**.

Each Respondent is solely responsible for ensuring that its response is delivered on time to the correct location.

In the event that a response is not sufficiently clear, the CSC reserves the right to seek additional information at their sole discretion.

2.9.1 Identification of Response: Each Respondent should ensure that its name, address, the request for information number and the closing date appear legibly on the outside of the response or as part of their cover page included in their email response.

2.9.2 Return of Response: Responses to this RFI will not be returned.

2.10 Procurement Strategy

This RFI is for the sole purpose of gathering information as described herein.

ANNEX A – Response Requirements

The following questions are key elements for which CSC is seeking feedback. Though respondents are invited to make any comments or suggestions freely, CSC requests that respondents comment specifically on the subjects addressed in the questions below. CSC also requests that respondents indicate the number of the questions listed below to which the responses pertain.

Answers can be submitted in one of the two official languages of Canada (English or French).

Since this RFI is not a request for proposal and since no contract will be awarded solely because of this RFI, Canada reserves the right to open and review the responses upon receipt, if Canada wishes to be able to consult the responders before the closing date.

This RFI is not a commitment with respect to future purchases or contracts. In preparing their responses, the Respondent community should refer to *ANNEX B – CSC Technical Environment Information*.

CSC is requesting that the Respondent community provide the following:

1. Corporate Profile

Each Respondent should provide:

a. Company name, address, telephone & fax numbers and e-mail address;
b. Company contact name and telephone number; and
c. Company background information including location of parent company, contact information for company representative and/or distributor in Canada (if any), types of products sold, and website address.

CSC may request additional contact information at any point in time.

2. Solution Description

Each Respondent should provide:

a. A Solution identifier such as a model number, version number and a description of all components required for the Solution;
b. Brochures including photos outlining full Solution specifications;
c. Details of the infrastructure components required to deploy the Solution;
d. Pricing model(s);
e. Licensing model(s); and
f. Support and maintenance model(s).

3. Questions to Industry

TABLE 1 – Object-oriented Data Models

1	Describe how the Respondent solution supports object-oriented data. a. In addition, please describe the type of database. b. What are the top use cases for the database (for example, analytical, transactional, operational, media, etc.)? c. Please describe how the database supports these top use cases.
2	Please provide examples where the database offering has been used for Master Data Management and/or as the authoritative source of data.
3	Describe the query functionalities offered by the database solution. When responding, please consider: a. The maturity level of the complex query functionality (for example, aggregate functions, sorting, grouping, etc) b. Full text search capabilities. c. Indexing capabilities; does it support unique indexing capabilities?
4	ACID Compliance: a. Please describe how the database provides support for ACID (Atomicity, Consistency, Isolation, and Durability), including scenarios where data is spread across multiple servers or nodes; b. Describe the approach(es) used to guarantee data consistency both across data sets or replicas and within a transaction; c. Describe how constraints such as uniqueness can be enforced in the database solution; d. Please describe how the database supports data modelling best practices.
5	Describe the concurrency control strategies used by the database. When responding, please explain: a. How data is reserved and released; and b. Impact of concurrency strategy on performance.
6	Please describe the horizontal partitioning capabilities of the database solution.

7	Please describe the data replication capabilities of the database and how this feature could be implemented in a Protected B cloud environment within one cloud provider region and across multiple regions. a. Describe the features and functionality used to ensure data consistency; b. Describe the data recovery capabilities available in case of failure; c. Describe the data replication capabilities and best practices in a hybrid landscape.

TABLE 2 – Security

8	The CSC solution must support the ability to securely handle Protected-B data both in transit and at rest. a. Please describe the encryption capabilities, protocols, strengths and recommended approaches to support this requirement; b. Please identify the Cipher Suites that the database solution supports; c. If possible, please indicate how the database solution complies with the Government of Canada Privacy Act and the National Cyber Security Strategy (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx).
9	Can the database operate as a PaaS on cloud infrastructure that is completely located and segregated to Canadian data centers? (Please refer to Annex C).
10	Auditing and Logging: a. Please describe how the database solution's audit and logging capabilities help to ensure the protection of personal information for Create, Read, Update and Delete events on all system objects (data, user accounts, roles, system configurations, etc.); b. Please indicate the default retention periods and whether the retention period is configurable by the client.

11	Please describe the proposed database solution information security policies, procedures, and security controls. As part of the description, please identify if the solution meets one or more of the following standards: • ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; • ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services; • AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality; and o 7:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services; and o AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality. • The Communications Security Establishment Canada (CSEC) Information Technology Security Guidance (ITSG) ITSG-33 control standards (https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)
12	Please describe what the proposed database solution offers as default and configurable services for Identity management and Access management.

TABLE 3 – Database Functionality and Performance

13	If available, please provide any third-party, industry-audited performance metrics for Create/Read/Update/Delete transactions for the database.
14	Please identify any database schema, document/record, or data element size restrictions.
15	Please describe if and how the database handles multiple creates / updates / deletes within a single transaction.
16	Please describe how the database manages Role Based Access Control (RBAC) capabilities, including the level of granularity natively supported in the solution (e.g.: schema, table or collection, element).
17	Please provide the database capabilities to offer scalability to easily and securely manage transaction growth.

18	Please describe the data types supported by the database: c. For each data type, please include the formats, predefined ranges, restrictions, and any limitations d. If not specified above, please identify the data types used to support large images and videos. Please include any blob size limitations.
19	Please describe the data type formats used to store date and time values across multiple time zones
20	Please describe the capabilities provided for schema enforcement and validation, including items such as data types and business rules.
21	Does the database offer the capability to perform queries based upon Geospatial data?
22	Does the database solution offer the ability to visually monitor DBMS processes, performance and workflows via dashboards (for example, performance, monitoring, management, etc.)? Please describe and provide samples.
23	Does the database solution offer tools to enable data visualization? Please describe and provide samples.
24	Please describe the database solution capabilities with respect to deployment automation.
25	Please describe the database solution capabilities with respect to AI/machine learning.
26	Does the Respondent provide a mobile version of the database and support data synchronization between mobile and a hosted solution?
27	Please describe the database backup capabilities and how they align with industry best practices.

TABLE 4 – High Availability

28	Please describe the database configuration strategy and solution capabilities for supporting high availability.
29	Please describe the database solution disaster recovery capabilities.

TABLE 5 – Data Migration and Data Sharing

30	As indicated in the Background section, CSC will be transitioning from a legacy to hybrid environment. a. Please describe the capabilities of the database solution in supporting large migrations of existing relational data; b. Please describe best practices in completing this type of data migration and switching systems of record.
31	Please describe the database capabilities, associated software tools, and best practices for synchronizing (real time or near real time) data between a Cloud solution and on premise legacy databases.
32	Please describe the database capabilities to share/ETL large data sets, either with third party Respondents or natively to a data warehouse.
33	Please provide examples of the Respondent assisting a past client with the following: a. Migrating data to the cloud; b. Supporting a hybrid solution comprised of relational on premise and cloud databases.

TABLE 6 – Enterprise Solution

34	Please describe the Respondent maintenance and support offerings (i.e., pre-deployment, post-deployment, consulting after-hours support, 7/24 on-call support, etc.) and how this support is provided.
35	If the Respondent provides a hosted solution, does the Respondent offer guaranteed minimum service levels though service level agreements (SLAs)? If so, please describe the SLA model.
36	Please describe the Respondent training offerings and resources.
37	General solution pricing: a. Please provide a summary of the database solution pricing structure b. If possible, within the pricing structure, please identify one-time costs versus on-going license, subscription, maintenance and support costs c. Please provide costing for various on-demand technology roles (for example, solution architects, DBAs, support specialists)

38	Please provide two use cases where the Respondent’s database solution has been implemented within large-scale cloud and hybrid environments. a. Include the implementation timeline, why the implementation was considered a success, and any major obstacles. b. If available, include a solution that supported a Protected B environment. c. If available, include a solution that has been implemented at a Government or Public Safety organization
39	Migrating from an on-prem distributed relational database environment to a Protected B cloud database solution comes with many risks. a. Based upon the information provided in this document, what significant risks does the Respondent foresee for this CSC project? Please provide a list of risks from the perspectives of planning, migration, implementation, and support. b. What steps does the Respondent recommend to mitigate those risks?
40	Please provide a product roadmap for the database solution identified in the response, including the release horizon and frequency of software updates.
41	Please provide a sustainability roadmap for the database solution identified in the response.
42	Please identify any industry recognized certifications for the proposed solution.
43	What other products or services does the Respondent provide that complement the solution?
44	Please indicate how the Respondent organization contributes to open source solutions and communities.
45	Please describe how the database supports the Government of Canada standards and directives as defined in 1.1.2.
46	Please identify if the Respondent is already on a Government of Canada approved standing offer or other procurement vehicle.

TABLE 7 – Data Management and Governance

47	Please describe Data Governance capabilities provided by the Respondent solution.
48	Please provide examples of the solution flexibility in managing relevant metadata.

4. Alternative Suggestions

Does the Respondent have any suggestions and/or concerns with respect to the questions listed in *Annex A* or the technical environment in *Annex B*? Are there any foreseeable issues that would prevent the Respondent from being able to respond to a future proposed bid solicitation? If so, please outline the Respondent's suggestion(s), concern(s) and any recommendations to resolve them.

5. Demonstrations

Would the Respondent be interested in attending an RFI follow-up session with the opportunity to demonstrate the Database solution? These sessions will take place on-site at CSC or remotely utilizing web/video conferencing. See the section entitled *Follow-up Activity* for more details.

ANNEX B – CSC Technical Environment Information

1. Data Sovereignty

The protection of information, from a privacy and security perspective, is core to the integrity of government programs, which underpins confidence in Canada. All information managed by Canada requires protection, including information published publicly in order to appropriately protect the confidentiality, integrity and availability of the information. The information up to and including "Protected B" may be shared while using the network, and it is incumbent that the work incorporates the appropriate controls in order to safeguard the interests of Canada and those of its partners to this level of security.

Furthermore, security controls, which ensure the confidentiality, integrity and availability of the work, are imperative requirements for the work alone monitoring system, as Canadians expect Canada to take all appropriate measures to protect personal and sensitive information. Therefore, the anticipated solution must be within the political and geographic boundaries of Canada (see *Annex D - Certification of Data Centres Located in Canada*). Stringent contractual and technical measures must be put in place to ensure that information is secured at all times, at rest and in motion, through encryption protection and is only accessed by those authorized to access the infrastructure for those purposes approved by Canada.

2. Data Privacy and Information Security

All CSC data must be managed in accordance with Canadian Security Establishment *IT Security Risk Management Life Cycle Approach (CSE ITSG-33).* It is anticipated that GC Security Control Profile for Cloud-based GC Services will be applicable for this requirement.

Canada will require the Respondent to establish and maintain a data privacy and information security program, including physical, technical, administrative, and organizational safeguards designed to:

a. Ensure the security and confidentiality of Canada's Data;

b. Protect against any anticipated threats or hazards to the security or integrity of Canada's Data;

c. Protect against unauthorized disclosure, access to, or use of Canada's Data;

d. Ensure the proper disposal of Canada's Data; and

e. Ensure that all employees, agents, and subcontractors of the Contractor, if any, comply with all of the foregoing.

3. Current Service Offering

3.1 Geographical Distribution

CSC's current OMS application is accessed across Canada consisting of five geographical regions and the National Headquarters.

3.2 Number of OMS Application Users

As of June 2017, Correctional Service of Canada had approximately 15,000 OMS application user accounts which included 14,000 CSC internal and 1,000 external users. CSC estimates that there are between 500-600 concurrent users at peak times, geographically disbursed across the country.

3.3 Number of Master Records

The solution holds information about approximately 100,000 past and current offenders. However some current offender business tables contain over 1 million records.

3.4 Current OMS Database Size

The current OMS application databases total approximately 1.1 terabytes in size, when adding all regions together. This size estimate does not include schema required to manage ETL processes or archive logs. There are approximately 230 transaction tables in the current relational database.

ANNEX C – Certification of Data Centres Located in Canada

By submitting a response, the Respondent acknowledges that the proposed Database solution must be capable of operating in a cloud native / on-premise environment that is located within a Canadian province or territory. The Respondent must also ensure that:

1. Data transmitted and/or stored by and for Correctional Service Canada (CSC) shall be segregated from all trans-border dataflow between Canada, the United States of America (USA) and other foreign countries;
2. Under no circumstance will the data be transmitted, stored or shared other than between the Respondent and CSC;
3. Data transmitted and/or stored by and for CSC shall be segregated from other company records and information holdings and shall be delivered to the Government of Canada upon request; and
4. Electronic audit trails for information are stored in an access controlled database in order to easily determine the history of access for any individual at any time.