cdic sadc

Canada Deposit Insurance Corporation | Société d'assurance-dépôts du Canada

REQUEST FOR SUPPLY ARRANGEMENT ("RFSA")

RFSA #2023-3941

1. Title

Information Technology Staff Augmentation and Project Delivery Services

2. Introduction

1. The Canada Deposit Insurance Corporation **("CDIC")** is seeking to establish a qualified pool of Suppliers to provide Information Technology ("IT") Staff Augmentation Services and IT Project Delivery Services as further described in Schedule "A" (Statement of Work) for any one or both of the following two (2) Service Streams:

   Service Stream #1: Staff Augmentation Services
   Service Stream #2: Project Delivery Services

   on an as and when required basis, for a three-year term.

   The Canada Deposit Insurance Corporation ("**CDIC**") will establish up to twenty (20) Supply Arrangements for Service Stream #1: Staff Augmentation Services and an unlimited number of Supply Arrangements for Service Stream #2: Project Delivery Services.

2. CDIC is a federal Crown corporation, with headquarters in Ottawa. CDIC is responsible for providing insurance against the loss of part or all of deposits, and for promoting and otherwise contributing to the stability of the financial system in Canada. These objectives are pursued for the benefit of persons having deposits with CDIC member institutions and in such a manner as will minimize the exposure of CDIC to loss. CDIC is also the resolution authority for CDIC member institutions.

   Further information about CDIC can be obtained at www.cdic.ca.

3. Trade Agreements

This procurement is covered by Chapter Nineteen (Government Procurement) of the Canada-European Union Comprehensive Economic and Trade Agreement (CETA) and Chapter Nineteen of the Canada-United Kingdom Trade Continuity Agreement (CANADA_UK TCA), and Chapter Five (Government Procurement) of the Canadian Free Trade Agreement (CFTA).

4. Summary of Key RFSA Dates

Request for Supply Arrangements	
Date of Issuance:	August 16, 2023
Deadline for Submission of Questions:	September 1, 2023, 2:00 p.m. Ottawa local time
CDIC Response to Questions:	By September 18, 2023
Deadline for Proposals:	October 4, 2023, 2:00 p.m. Ottawa local time
Anticipated Ranking and Commencement of Negotiations	October 20, 2023
Contract Negotiation Period	Thirty (30) business days
Anticipated Award Date:	On or about October 12, 2023
Proposal Validity Period:	120 days from Deadline for Proposals
Proposal Delivery Address:	procurement@cdic.ca
CDIC Procurement Advisor:	Judy Ann Hollander

Note: The RFSA timetable above is tentative only and may be changed by CDIC at any time.

5. Incorporated Schedules and Appendices

In addition to the main body of this RFSA, the following schedules and appendices are included as part of the RFSA:

Goods and Services Requirements:	See Schedule "A" (Statement of Work)
Evaluation and Selection:	See the main body of this RFSA and: • Schedule "B" (Evaluation and Selection Process) • Schedule "C" (Technical Offer Submission Form) • Appendix "C-1" (Technical Offer) • Appendix "C-2" (Reference Engagement Form) • Schedule "D" (Financial Offer Requirements and Evaluation) • Appendix "D-1" (Financial Offer Submission Form) • Appendix "D-2" (Financial Offer for Service Stream #1)
Required Forms:	See the main body of this RFSA and Schedule "E" (Required Forms)
Form of Agreement:	See this RFSA and Schedule "F" (Form of Professional Services Agreement)
Term of Agreement:	Three (3) year term

6. Questions and Communication Related to the RFSA Document

1. Any questions or requests for clarification of the contents of, or interpretation or correction, relating to this RFSA must:

   i) be made in writing prior to the Deadline for Submission of Questions;
   ii) be submitted by electronic mail to the Proposal Delivery Address and addressed only to the CDIC Procurement Advisor.

2. Answers to questions will be made available as written addenda to this RFSA no later than the Deadline for CDIC Response to Questions, in the same manner as the RFSA.

3. Any attempt by a bidder or any of its employees, agents, contractors or any other representatives to contact any person at CDIC other than the CDIC Procurement Advisor, or to contact the CDIC Procurement Advisor regarding this RFSA, other than in writing at the Proposal Delivery Address, may in CDIC's sole and absolute discretion, result in the bidder's disqualification and the rejection of its Proposal.

4. Nothing in this RFSA limits CDIC's right, in its sole and absolute discretion, for which CDIC shall have no obligation, to communicate with any bidder regarding any matter in the normal course of business from any contractual relationship for the provision of any other or similar goods or services independently of this RFSA.

5. It is the sole responsibility of a bidder to avail itself of any information it may require, ask any questions, or obtain any clarification of the requirements or other matters in this RFSA, and make its own investigations, projections and conclusions prior to submitting a proposal.

7. Proposal Delivery

1. Proposals must be received in electronic format at the Proposal Delivery Address no later than the Deadline for Proposals. It is the bidder's responsibility to ensure that the proposal is delivered by the Deadline for Proposals to the Proposal Delivery Address. The time of delivery shall be the time the email is received in the inbox of the email address provided as the Proposal Delivery Address.

2. Proposals received after the Deadline for Proposals may be deemed to be non-compliant. CDIC may, in its sole and absolute discretion, accept a Proposal delivered to the Proposal Delivery Address after the Deadline for Proposals if CDIC deems it to be in CDIC's best interests, and the bidder demonstrates to CDIC's satisfaction that:

   i) the Proposal would have been delivered to the Proposal Delivery Address by no later than the Proposal Submission Deadline but for circumstances beyond the bidder's control; and
   ii) CDIC's acceptance of the Proposal would not otherwise confer a substantive advantage on the bidder.

3. CDIC may only accept Proposals submitted to the Proposal Delivery Address. Proposals submitted by another means or at any other physical location (as applicable) may be deemed by CDIC to be non-compliant and rejected.

4. Bidders may, in writing, revoke and re-submit a proposal at any time up to the Deadline for Proposals.

---

8. Proposal Format

1. Proposals are to be submitted in either English or French to the Proposal Delivery Address, as follows:

   i) in Adobe Reader format (.pdf).
   ii) the "**Technical Offer**", responding to the technical requirements set-out in Appendix "C-1" (Technical Offer) and Appendix "C-2" (Reference Engagement Form); and
   iii) The "**Financial Offer**", responding to the financial requirements set-out in Schedule "D" (Financial Offer Requirements and Evaluation) and if applicable Appendix "D-1" (Financial Offer for Service Stream #1), shall be submitted as a separate attachment.

   The maximum file size which CDIC is able to receive via email is 20 MB. There is no limit to the number of attachments that may be submitted. It is highly recommended to contact the CDIC Procurement Advisor in a separate email to the Proposal Delivery Address to confirm CDIC's receipt.

---

9. Proposal Requirements and Required Documents

1. Bidders may submit Proposals for any one or both of the Service Streams.

2. Bidders must comply with all requirements of this RFSA, including those identified as "must" or "shall", including, but not limited to, the requirement to:

   i) submit information in support of each Rated Requirement listed in Appendix "C-1" (Technical Offer) and Appendix "C-2" (Reference Engagement Form); and
   ii) submit a Technical Offer (including all forms listed in Schedule "E" (Required Forms)), completed as required.

3. Where a bidder fails to include any of the required information or documents in its Proposal, CDIC may, in CDIC's sole and absolute discretion (but provided that it treats all bidders in the same manner):

   i) require the submission of such information or documents within a prescribed timeframe satisfactory to CDIC; and
   ii) reject or refuse to consider any Proposal from a bidder who fails to comply with any such submission requirement.

---

10. Evaluation and Selection

Proposals will be evaluated in accordance with the evaluation and selection process set out in Schedule "B" (Evaluation and Selection Process).

The successful bidders will be notified via email to the contact person at the email address provided by the bidder in Schedule "C" (Technical Offer Submission Form). Following the award of Supply Arrangements resulting from this RFSA, CDIC will publish an Award Notice on www.CanadaBuys.Canada.ca (or such other electronic tendering service utilized by CDIC at the relevant time) and will inform unsuccessful bidders via email.

---

11. CDIC's Reserved Rights

Notwithstanding anything to the contrary in this RFSA, CDIC reserves the right, in its sole and absolute discretion, to exercise any or all of the following rights, alone or in combination with each other, to:

1. Evaluate or accept Proposals:

   i) which in CDIC's sole and absolute discretion substantially comply with the requirements of this RFSA; or
   ii) in whole or in part without negotiations.

2. Enter into negotiations with:

   i) any or all bidders on any or all aspects of their Proposal; or
   ii) any or all bidders, or any prospective persons or entities capable of delivering the required services but who may not have submitted a proposal in response to this RFSA in the event, in CDIC's sole and absolute discretion, no proposals meet the requirements of this RFSA.

3. Conduct a best and final offer process:

   i) with any or all bidders in which bidders are invited to revise their financial offers in circumstances where CDIC deems appropriate in CDIC's sole and absolute discretion.

4. Cancel, modify, re-issue or suspend:

   i) any aspect of this RFSA, in whole or in part, at any time, for any reason;
   ii) the schedule for this RFSA, including without limitation the Proposal Submission Deadline stated above and any other activity or date stipulated in this RFSA, in whole or in part, at any time, for any reason; or
   iii) this RFSA in its current or modified form and invite proposals from only the bidders who submitted proposals in response to this RFSA, where to do so is deemed, in CDIC's sole and absolute discretion, to be in CDIC's best interests.

5. Seek clarification, validate or take into account:

   i) independently or with the help of the bidder, any or all information provided by the bidder with respect to this RFSA and, for this purpose, disclose any or all

information provided by the bidder to a third party, subject to CDIC obtaining appropriate assurances of confidentiality from those third parties.

6. Reject or refuse to consider any proposal (or otherwise exclude a bidder that submitted any proposal):

   i) if, in CDIC's sole and absolute discretion, it fails in any material respect to comply with the requirements of this RFSA;
   ii) containing false, misleading or misrepresented information;
   iii) in the event any matter causes or is likely to cause, in CDIC's sole and absolute discretion, a conflict of interest in relation to the selection of any proposal;
   iv) from a bidder who colludes with one or more other bidders in the preparation of any proposal;
   v) from a bidder who fails to cooperate with CDIC in any attempt by CDIC to clarify or validate any information provided by the bidder or who fails to provide accurate and complete documentation as directed by CDIC;
   vi) from a bidder against whom economic sanctions have been imposed by the Government of Canada;
   vii) from a bidder with whom CDIC has previously terminated an agreement for any reason, or currently has a commercial or legal dispute that, in CDIC's sole and absolute discretion, would impair CDIC's ability to enter into the productive business arrangement contemplated by this RFSA;
   viii) from a bidder failing to have the capacity to contract with CDIC, or Her Majesty, or both;
   ix) if deemed by CDIC, in its sole and absolute discretion, as necessary to safeguard Canada's security interests or if the bidder is prohibited from receiving any benefits under an agreement between Her Majesty and any other person by virtue of Section 750(3) of the *Criminal Code of Canada*;
   x) from a bidder on any of the following grounds: (i) bankruptcy or insolvency; (ii) false declarations; (iii) significant or persistent deficiencies in performance of any substantive requirement or obligation under a prior contract or contracts; (iv) final judgments in respect of serious crimes or other serious offences; (v) professional misconduct or acts or omissions that adversely reflect on the commercial integrity of the bidder; or (vi) failure to pay taxes;
   xi) if it contains rates or prices that are considered to be, in CDIC's sole and absolute discretion, commercially unreasonable; or
   xii) if, in CDIC's sole and absolute discretion, it contains a mathematical error(s) that results in any discrepancy, inconsistency, vagueness, ambiguity, uncertainty or conflict related to prices which affects the integrity of the procurement process.

7. Award:

   i) One or more non-exclusive Professional Services Agreements in connection with this RFSA.

8. Waive:

   i) irregularities, informalities, non-conformity, non-compliance, omissions and defects in any proposal where, in CDIC's sole and absolute discretion, they do not materially affect the ability of the bidder to provide the goods or services required by this RFSA.

9. Correct:

   i) mathematical errors in Financial Offers.

The exercise of any of the above rights or sub-rights of CDIC shall not be a waiver or limit the right of CDIC to exercise any other rights.

12. Limitation of Liability

1. By submitting a proposal, the bidder acknowledges and agrees to the requirements of this Section 12.

2. Bidder acknowledges and agrees that in no event shall CDIC, its employees, officers, directors, consultants or advisors be liable or responsible for:

   i) any damages, including without limitation direct, indirect, consequential, incidental, general, special or exemplary damages, any economic losses, any lost profits, opportunities, expenses, costs or any other losses (collectively, the "Consequential Losses") arising out of, in connection with, or in any way related to, any bidder's participation in this RFSA or any acts, omissions or errors, including negligence of, or breach of contract by CDIC, its employees, officers, directors, consultants and advisors; or
   ii) any actions of any bidder in relation to CDIC, or another bidder, or any third party, in receiving and responding to this RFSA.

3. Without limiting the above, expenses or costs incurred by any bidder in any way related to or associated with this RFSA, including without limitation the preparation, submission or evaluation of proposals, the provision of information to CDIC or CDIC's authorized representative for a determination of any bidder's technical, managerial or financial capabilities, any expenses related to travel, and the satisfaction, fulfillment or completion of any conditions precedent to any agreement with CDIC to deliver the goods and services required by this RFSA, are a bidder's sole responsibility and may not be charged to CDIC in any way.

4. Without limiting any rights CDIC may reserve elsewhere in this RFSA or may have otherwise at law, CDIC may, in its sole and absolute discretion, elect to exercise its sole and absolute discretion pursuant to this RFSA, without any liability or obligation to any bidder.

5. If any bidder is determined by a court or trade tribunal of competent jurisdiction to be entitled to compensation arising from this RFSA or from the actions of CDIC, its employees, officers, directors, consultants or advisors in relation to this RFSA, including without limitation any exercise of CDIC's sole and absolute discretion, the bidder expressly acknowledges and agrees by submitting a proposal that the aggregate amount of compensation said bidder would be entitled to for, without limitation, any and all damages, opportunities, expenses, costs, or other losses, including Consequential Losses, either individually or cumulatively, is limited to one thousand dollars ($1,000.00 CAD).

13. Governing Law

This RFSA is governed by and construed in accordance with the laws in force in the Province of Ontario, Canada, and, subject to the jurisdiction of the Canadian International Trade Tribunal, Ontario courts have exclusive jurisdiction to hear any disputes under this RFSA.

14. Resulting Agreements and Term of Agreement

1. CDIC intends to award Supply Arrangements based on Schedule "F" (Form of Professional Services Agreement).

   Each such Professional Services Agreement will include:

   i) the form of Professional Services Agreement (attached to this RFSA as Schedule "F" (Form of Professional Services Agreement);

ii) the applicable portion(s) of the Statement of Work, attached to this RFSA as Schedule "A" (Statement of Work);
iii) any other RFSA document CDIC deems appropriate to include as part of the resulting agreement(s); and
iv) the applicable documents submitted with the successful proposal.

2. CDIC intends to have Professional Services Agreements in place with successful bidders within fifteen (15) business days of being notified of having been selected as a successful bidder.

3. Once CDIC has entered into a Professional Services Agreement with at least one (1) successful bidder, CDIC may, in its absolute discretion, begin requesting services from any such firm, whether or not any Professional Services Agreements have yet been entered into with other successful bidders.

4. CDIC reserves the right, in its sole discretion, to award additional Supply Arrangements to ensure all Service Categories/Roles under a Service Stream are covered across any resulting Professional Services Agreements and ensure CDIC's operational requirements are met.

---

15. Debriefing

After notification of the results of this RFSA process, bidders may request a debriefing. Bidders should make the request to the CDIC Procurement Advisor within twenty-one (21) calendar days of receipt of the notification. The debriefing may be in writing, by telephone or by video conference. The intent of the debriefing information session is to aid bidders in understanding why their proposal was not selected. Any debriefing provided is not for the purpose of providing unsuccessful bidders with an opportunity to challenge the procurement process.

---

16. No Guarantee of Volume of Work or Exclusivity of Contract

CDIC makes no guarantee of the value or volume of work Supply Arrangement (SA) Holders may receive through the Supply Arrangement. The value and volume of Services, if any, acquired will depend on a variety of factors including annual budgetary approvals.

The Professional Services Agreement executed with SA Holders will not be exclusive contracts for the provision of the described Services. CDIC may contract with others for the same or similar services to those described in this RFSA or may obtain the same or similar services internally.

---

17. Disclaimer

CDIC makes no representation or warranty as to the accuracy or completeness of any information provided by it in connection with this RFSA and disclaims all express and implied representations, warranties, and conditions in connection with this RFSA.

Bidders should make their own investigations, projections and conclusions. Bidders should consult their own advisors to verify independently the information contained in this RFSA and to obtain any additional information that they may require, prior to submitting a proposal.

18. General

1. In the event of any discrepancy, inconsistency or conflict between the wording of the English or French version of this RFSA, or any related documents, the wording of the English version shall prevail.

2. CDIC agrees to keep in confidence any information contained in a Proposal that is clearly marked "confidential". Notwithstanding the foregoing, the submission of a proposal by a bidder constitutes an acknowledgement by that bidder that CDIC is subject to the *Access to Information Act* (Canada), as amended from time to time, and that, as a consequence, CDIC may be required to disclose certain information contained in its records pursuant to a request for access made under that Act.

3. CDIC requires any persons supplying services to or performing any work for CDIC to conduct their affairs to avoid any conflict of interest. A conflict of interest includes any situation where a bidder has or may have an unfair advantage or where other commitments, relationships or interests could or could be seen to compromise a bidder's performance of its obligations to CDIC. To the extent that a bidder may be in a conflict of interest, that bidder must include a description of such conflict of interest in its Proposal.

   If CDIC is of the belief that a bidder may be in a conflict of interest, CDIC may disqualify the proposal submitted by the bidder or terminate any agreement with that bidder pursuant to this RFSA.

---

19. Not a Tender, No "Contract A / Contract B"

This RFSA is not an offer to enter into either a binding contract (often referred to as "Contract A") or an agreement to acquire goods or services from the bidder (often referred to as "Contract B"). Neither this RFSA nor a bidder's proposal shall create any contractual rights or obligations whatsoever on any of CDIC or any bidder, save and except related to limitation of liability.

Bidder proposals are revocable by bidders; however, CDIC is under no obligation to continue to evaluate or consider any proposal that the bidder seeks to modify following the Deadline for Proposals (including any change in pricing that is adverse to CDIC). Proposals and related information about bidders will be assessed during the evaluation of Proposals and accordingly, misleading or incomplete information, including withdrawn or altered proposal information or pricing, could adversely impact any such evaluation, or result in CDIC revisiting that evaluation and may result in disqualification, in CDIC's sole discretion.

[END OF MAIN RFSA BODY]

Schedule "A"

Statement of Work

DEFINITIONS

Capitalized terms used in Schedule "A" (Statement of Work) are either defined below or in the Professional Services Agreement attached as Schedule "F" (Form of Professional Services Agreement) to this RFSA.

"Bidder" means an entity submitting a Proposal, or who is considering submitting a Proposal in response to this RFSA;

"**Engagement**" means a specific body of work that was carried out pursuant to a specific client requirement/need;

"**Financial Offer**" consists of the fillable forms contained in Appendix "D-1" (Financial Offer Submission Form).

"**Professional Services Agreement**" or "**PSA**" means the agreement to be entered into by a successful bidder with CDIC, for any one or all of the Service Streams (see Schedule "F" (Form of Professional Services Agreement));

"**Proposal**" means the Technical Offer submitted by a Bidder when applying for the Supply Arrangement under this RFSA;

"**Reference Engagement**" means an Engagement, the details of which are being provided by a Bidder as evidence of the Bidder's technical experience and expertise;

"**Reference Engagement Form**" means the fillable form contained in Appendix "C-2" (Reference Engagement Form);

"**RFSA**" means this Request for Supply Arrangement #2023-3941;

"**Role**" means, for purposes of this RFSA, any one role identified in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles) of this RFSA.

"**Service Category**" means, for purposes of this RFSA, any one service category identified in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles) and/or Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories) of this RFSA.

"**Service Request**" means a document issued by CDIC to an SA Holder(s), that includes instructions and applicable CDIC service requirements, which may result in a Task Authorization. (See Section 4, Service Request Process of Schedule "A" (Statement of Work));

"**Service Stream(s)**" means the services identified as Service Stream #1: Staff Augmentation Services, and/or Service Stream #2: Project Delivery Services, as described in Schedule "A" (Statement of Work);

"**SLA**" means service level agreement;

"**Supply Arrangement**" means an arrangement entered into between a successful bidder and CDIC by executing a Professional Services Agreement;

"**Supply Arrangement Holder**" or "**SA Holder**" means a successful bidder that has entered into a Professional Services Agreement under this RFSA;

"**Task Authorization"** means the authorization issued by CDIC, following the receipt of an SA Holder's response to a Service Request, authorizing services to be completed under the Supply Arrangement; and

"**Technical Offer**" consists of the fillable forms contained in Schedule "C" (Technical Offer Submission Form), Appendix "C-1" (Technical Offer); and Appendix "C-2" (Reference Engagement Form).

1. TITLE

Information Technology Staff Augmentation and Project Delivery Services

2. BACKGROUND

CDIC was established in 1967 by the *Canada Deposit Insurance Corporation Act* (Canada). It is a federal Crown corporation named in Part I of Schedule III to the *Financial Administration Act* (Canada). The Corporation reports to Parliament through the Minister of Finance.

CDIC is responsible for providing insurance against the loss of part or all of deposits, and for promoting and otherwise contributing to the stability of the financial system in Canada. These objectives are pursued for the benefit of persons having deposits with CDIC member institutions and in such a manner as will minimize the exposure of CDIC to loss. CDIC is also the resolution authority for CDIC member institutions.

In furtherance of its statutory mandate, CDIC performs certain core functions with respect to member institutions which include:

a) Validation and continued testing of member institution compliance with data standards and system requirements;

b) Calculation of deposit liability and collection of insurance premiums from member institutions to provide an adequate level of insurance protection for Canadians' eligible deposits;

c) Proactive and continued risk monitoring and, where necessary, timely intervention at member institutions; and

d) Assessing, determining and administering appropriate payouts of eligible insured funds to depositors, where appropriate.

In support of its mandate, CDIC's information systems continue to evolve and increase in complexity in order to support CDIC's business requirements. As CDIC's reliance on technology continues to expand, investments to ensure the stability and integrity of systems and security of information will persist. As such, CDIC is continuing to improve its Information System (IS) service delivery model, ensuring that IS resources are strategically aligned with operational requirements and deliver efficiently and effectively.

3. OBJECTIVES

3.1 The purpose of this RFSA is to establish a three (3) year Supply Arrangement vehicle with experienced and qualified firms capable of delivering the information technology staff augmentation and project delivery services, under one or multiple Service Streams described herein, on an as and when required basis.

4. SCOPE

4.1 The types of Services required for this RFSA include, but are not limited to the following two (2) Service Streams:

- Service Stream #1: Staff Augmentation Services
- Service Stream #2: Project Delivery Services

The Services described below are meant to provide a high-level framework of the services. The actual scope, deliverables, qualifications and requirements for the Services will be identified at the time of the requirement and further defined in a Service Request.

NOTE TO BIDDERS: Bidders may submit a Technical Offer for one or more Service Streams, as described in Schedule "B" (Evaluation and Selection Process). The Statement of Work in the resulting Professional Services Agreement will be modified by CDIC based on the Service Stream(s) awarded to a bidder as a result of this RFSA. A bidder awarded a Professional Services Agreement in any of the foregoing Service Streams is a Supply Arrangement Holder (SA Holder) for the purpose of that Service Stream.

5. DESCRIPTION OF SERVICES FOR EACH SERVICE STREAMS

In order for a Bidder to be qualified to become an SA Holder under this Supply Arrangement, the bidder must qualify to provide Services in one or both of the following two (2) Service Streams by qualifying for at least one Service Category, (as set out in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles) and Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories*)*, under the Service Stream(s), for which the Bidder wishes to qualify.

5.1 Service Stream #1: Staff Augmentation Services

Service Stream #1 may include, but is not limited to, the following tasks, activities and/or deliverables, as further described in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles):

i. cover temporary absence of CDIC resources (e.g., due to leave), or:
ii. provide targeted support to on-going services or special projects where additional resources may be required.

Service Categories and Roles

The Service Categories and Roles of resources that CDIC may request under this Service Stream include those listed in Appendix "A-1" (Service Stream #1: Staff Augmentation Services*,* Service Categories and Roles), attached to and forming part of this Schedule "A" (Statement of Work).

Scope of work and deliverables will be specified in any resulting Service Request and will generally align with the job activities / responsibilities provided in Appendix "A-1" (Service Stream #1: Staff Augmentation Services, Service Categories and Roles).

5.2 Service Stream # 2: Project Delivery Services

Service Stream #2 may include, but is not limited to, the following tasks, activities, and/or deliverables, as further described in Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories):

i. work alongside CDIC to define the project approach, methodology, pricing and assignment of supporting resource(s) in compliance with CDIC's overall policies and procedures.
ii. incorporating agile methodologies into the project delivery life cycle to deal with on-going changes in the business and external environment.
iii. support through all phases of the project life cycle with application of appropriate project management techniques.

Project-specific scope of work and deliverables will be specified in any resulting Service Request and will generally align with the categories identified in Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories). Some of the projects may comprise of routine, ongoing activities while others may be required on a recurrent or ad-hoc basis.

Service Categories

The Service Categories that CDIC may request under this Service Stream include those listed in Appendix "A-2" (Service Stream #2: Project Delivery Services, Service Categories), attached to and forming part of this Schedule "A" (Statement of Work).

6. ALLOCATION OF REQUIREMENTS AND SERVICE REQUEST PROCESS

6.1 Without limitation to Section 2.1 of Appendix "A" (Services and Fees) of the Professional Services Agreement (attached as Schedule "F" (Form of Professional Services Agreement), requirements for Services will be procured by CDIC through a Service Request process, as may be amended from time to time, in CDIC's sole and absolute discretion:

6.1.1 Requirements for Services of an estimated dollar value **equal or less than seventy-five thousand dollars ($75,000)**, excluding applicable taxes may be directed by CDIC, in its sole and absolute discretion, to any one (1) SA Holder or to a party other than a SA Holder under an alternate Supply Arrangement or other arrangement to provide similar services.

6.1.2 For any requirements for Services of an estimated dollar value **greater than seventy-five thousand dollars ($75,000)**, excluding applicable taxes, CDIC shall, by way of Service Request, invite multiple SA Holders to respond to the Service Request, in accordance with their respective Supply Arrangement, to provide the Services, describing the requirements of a specific engagement, including the required timeframe to respond. SA Holders shall respond to the Service Request by the prescribed deadline and CDIC shall have no obligation to consider any Service Request Response that is received after the specified Service Request Response deadline. Only SA Holders qualified under this Supply Arrangement may be issued a Service Request, and are eligible to respond, at no charge to CDIC.

6.2 The Service Request may include such information as, but not limited to, the following, as may be applicable for each requirement:

A. Service Stream #1: Staff Augmentation Services:

i. Number of resource(s), role(s), and level(s) required;
ii. The minimum qualification requirements for the required role(s);
iii. The overall scope of work and any tasks specific to any resource role(s);
iv. The schedule and duration of the work assignment, including renewal options;
v. Location and hours of work;
vi. Any technology requirements specific to the work;
vii. Any Deliverable(s);
viii. Any Security requirements, including personnel, facilities, data and/or technology; and
ix. Any other requirements related to the Services.

B. Service Stream #2: Project Delivery Services:

i. The overall scope of work and any required tasks;
ii. Deliverables;
iii. Minimum qualification requirement for the project team;
iv. The duration of the engagement, including renewal options;
v. Any specific service levels;
vi. Any additional technology requirements specific to the Services;
vii. Any Security requirements, including personnel, facilities, data and/or technology; and
viii. Any other requirements related to the Services.

A sample Service Request Form and Task Authorization Form is provided in Appendix "D" (Sample Service Request and Task Authorization Form) to Schedule "F" (Form of Professional Services Agreement).

6.2.1 The Service Request will specify any other information to be included in the SA Holder's response, such as the name(s) and resume(s) of proposed resource(s), as well as outline the basis of the evaluation methodology and SA Holder selection. CDIC will evaluate responses and will select a successful SA Holder in accordance with the evaluation and selection process set-out in the Service Request. If an SA Holder responds to a Service Request, it will do so at no charge to CDIC.

6.2.2 The duly signed Service Request is the Task Authorization, authorizing the successful SA Holder to proceed with the performance of the Services in accordance with the agreed upon Service Request response.

6.2.3 Amendments to Task Authorizations: Any change or amendment to a Task Authorization will not be valid unless and until made in writing by means of a Task Authorization Amendment signed by CDIC and the SA Holder, which expressly amends the applicable Task Authorization.

7. NO VOLUME GUARANTEE

7.1 Services performed under the Supply Arrangement will be on an "as and when required" basis. CDIC makes no commitment or representation that a minimum level of business or any level of business will result from a Supply Arrangement. CDIC does not imply, represent nor warrant that it will require the SA Holder's services at any time.

8. REPORTING AND INVOICING REQUIREMENTS

8.1 SA Holders will be responsible for contract management activities related to any active Task Authorizations, including, but not limited to, tracking of hours, fees and burn rate, as to ensure Services delivered do not exceed the dollar amount approved in any Task Authorization.

SA Holders will provide a monthly report to CDIC on all active Task Authorizations, as required, including, but not limited to:

a) Status of work and any pending end dates, including all related applicable Task Authorization reference numbers provided by CDIC;
b) The name(s), role(s) and overall volume of resources engaged, and effort expended including detailed timesheets for each resource;
c) A detailed invoice to be submitted to CDIC no later than five (5) Business Days following month end, and which includes a summary of the services provided in the preceding month, supporting documentation in the form of detailed timesheets, and the related purchase order number(s) and Task Authorizations number(s);
d) For Task Authorizations that include a task/engagement specific SLA with CDIC, the SA Holder should report on its delivery of services against the identified SLA(s) within its monthly report; and
e) Performance under any vendor performance management framework, including monitoring of resource turnover, and any issues and resolutions required, where applicable.

9. LANGUAGE REQUIREMENTS

9.1 SA Holders must be able to provide resources who are proficient in English, at a minimum, and in some cases may be asked to provide bilingual resources who are also proficient in French. CDIC will specify the language requirements in the Service Request.

10. LOCATION OF WORK AND WORK HOURS

10.1 The location of work will be identified in the Service Request. The determination as to whether the work must be performed on-site or remotely will be at CDIC's sole discretion. Where CDIC determines that the work must be performed at CDIC's offices, CDIC will advise whether the work is to be performed at its office in Ottawa, Ontario, or its office in Toronto, Ontario. In either case, CDIC is not responsible for, and will not reimburse any travel or accommodation expenses.

10.1.1 No Personal Information or other Confidential Information or data may leave CDIC premises or be transferred to any third party or be transferred outside of Canada.

10.1.2 SA Holders may back-up information on servers outside of Canada except where the information is classified as "Protected B". "Protected B" information must remain within Canada.

10.2 Specific work hours will be included with any resulting Task Authorization. Notwithstanding, service requirements will generally be within the following timeframe, which is applicable to both the Ottawa and Toronto locations:

a. Business Hours: 7-hour day (or portion thereof), between the hours of 8 a.m. to 6 p.m., Monday to Friday (except Statutory Holidays); and

b. Off-Hours: CDIC anticipates that there may be some requirements for service delivery outside of the primary hours described above. Such requirements may arise as a result of critical project deadlines, requirement for system patches, or other operational requirements. CDIC will provide reasonable advance notice to the SA Holder of any such requirement. Any service delivery authorized by CDIC to be completed outside of the primary hours described above will be paid on the basis of hours actually worked, in accordance with the SA Holder's rate(s) for resource Roles (as accepted by CDIC); with no allowance for over-time.

11. SECURITY CLEARANCE

11.1 SA Holders must be able to supply and assign resources who are legally entitled to work in Canada, and that possess a valid security clearance granted by the Industrial Security Program of Public Works and Government Services Canada at the Reliability Status level, at a minimum, for work under any resulting Service Request.

11.2 CDIC will validate/confirm that all resources assigned to provide services under a Service Request possess the applicable security level required prior to authorization of any services to be rendered under a Service Request. Resources not currently in possession of a valid security clearance will need to obtain the required security clearance prior to commencement of any work.

12. RESOURCE AVAILABILITY AND SUBSTITUTION

12.1 SA Holders should ensure that any resources proposed and deployed in response to any issued Task Authorization remain available for the duration of the work period stipulated in the Task Authorization, unless resource becomes unavailable due to circumstances beyond the SA Holder's control (such as, but not limited to, illness, termination of employment with the SA Holder, or compassionate leave).

12.1.1 No resource substitution by the SA Holder may be permitted without CDIC's prior written consent and approval. Any alternate resource(s) proposed by the SA Holder must be deemed equivalent by CDIC, in its sole and absolute discretion. Where no equivalent alternate resource is available, CDIC reserves the right, in its sole and absolute discretion, to terminate a Task Authorization.

12.1.2 CDIC reserves the right to require the SA Holder to replace any deployed resource(s) should a resource not meet CDIC's qualification requirements and/or performance expectations.

13. VENDOR PERFORMANCE MANAGEMENT

13.1 CDIC is intending to implement a vendor performance management process. This process may consist of new metrics, tools, reports, processes and remedies designed to effectively and efficiently measure, report on and manage the level and quality of service being provided to CDIC.

13.2 SA Holders will be expected to comply with the vendor performance management guidelines that may be issued from time to time.

13.3 Should changes to performance management reporting and processes be implemented during the term of the Supply Arrangement, the SA Holders shall cooperate fully with CDIC in providing the information required and adapting existing processes to reflect the changes resulting from the implementation of these enhancements.

[END OF SCHEDULE "A" (STATEMENT OF WORK)]

Appendix "A-1"

Service Stream # 1: Staff Augmentation Services, Service Categories and Roles

CDIC may require resources to have additional skills or subject matter knowledge for specific engagements.

The following three (3) levels apply to all Roles in this RFSA (unless otherwise specified):

Level 1: Resource with basic/junior experience in successfully performing the Role.
Level 2: Resource with intermediate experience in successfully performing the Role.
Level 3: Resource with advanced experience in successfully performing the Role.

The following is a list of the ten (10) Service Categories applicable to this Service Stream.

#	Service Category
1	Advisory Services
2	Project Management
3	Cyber Security
4	Enterprise Technology
5	Technical Support
6	SharePoint Support
7	Alteryx Support
8	Application Development
9	Business Intelligence and Analytics
10	ServiceNow Development

The following is a list of the forty-five (45) Roles for Service Stream #1: Staff Augmentation Services, applicable to this RFSA, and are further defined below.

Role #	Service Category #1 - Advisory Services
1	IT Executive Strategic Advisor
2	Data Strategy Advisor

Role #	Service Category #2 - Project Management
3	Project Management Office Lead
4	Project Manager
5	Project Administrator / Coordinator

	Service Category #3 - Cyber security
6	Security Analyst
7	Application Security Administrator
8	IT Security Architect
9	Ethical / White Hat Hacker (or Penetration Tester)
10	Azure Security Architect
11	Azure Security Administrator
12	Cyber Forensics Specialist
13	Security Engineer (Application/Network)
14	SOC Analyst
15	SOC Lead/Manager
16	Cloud Security Specialist
17	Security Administrator
18	Governance Risk and Compliance (GRC) Analyst

Role #	Service Category #4 - Enterprise Technology
19	Storage Administrator / Virtualization Architect
20	Systems Architect (Network, Data, Applications)

21	Azure Architect
22	Azure Administrator
23	Azure Data Base Administrator
24	Webmaster

Role #	Service Category #5 - Technical Support
25	Application Support Specialist
26	Deskside Technical Support Analyst
27	Service Desk Analyst
28	IT Service Management Specialist
29	Infrastructure Operations and Support
30	Technical Writer / Trainer / Courseware Author (Developer)

Role #	Service Category #6 - SharePoint Support
31	SharePoint Online Administrator
32	SharePoint Online Architect
33	SharePoint Online Developer

Role #	Service Category #7 - Alteryx Support
34	Alteryx Developer

Role #	Service Category # 8 - Application Development
35	Solution Architect
36	Business Analyst
37	Application Developer
38	Azure Cloud Application Developer
39	Quality Assurance (QA) Tester

Role #	Service Category #9 - Business Intelligence and Analytics
40	Business Intelligence Developer
41	Data Architect
42	Data Scientist

	Service Category #10 – ServiceNow Development
43	ServiceNow Developer
44	ServiceNow Implementation Specialist
45	ServiceNow Solution Architect

1. The following are the specific descriptions for each Role in Service Category #1 – Advisory Services:

Role #1 - IT Executive Strategic Advisor
Responsibilities:
a) Provide vision and leadership in delivering on the strategic goals of CDIC by establishing the IT department's vision and mission and leading the implementation of the IT Strategic Plan; b) Develop an intimate understanding of CDIC's strategy and services to provide expertise on how to build and deploy scalable technology during expansion in the core and new business models; c) Ensure that architecture, governance and assurance exist, remove inefficiency in processes and champion standards that support business objectives and enable IT transformation; d) Ensure the security of the business, its staff and customers, as well as IT assets; e) Advise Senior Management on strategic system conversions and integrations in support of business goals and objectives; f) Be at the forefront of technology, assessing new computing technologies to determine potential value for the corporation; g) Manage and continuously adapt the future-state enterprise architecture;

h) Manage the IT budget and develop IT capital investment plans for implementing IT initiatives from the IT Roadmap and Strategic Plan;
i) Ensure that leading practices for IT governance, security, operations, development, projects and risk management are leveraged and practiced within IT and across the broader organization;
j) Manage relationships with strategic IT partners and vendors; and
k) Establish relevant and appropriate metrics and monitor and continuously improve service delivery performance.

Minimum Qualifications:

a) An undergraduate degree in Business, IT or a related discipline; and
b) Experience in a business and strategic advisory role within IT.

Role #2 - Data Strategy Advisor

Responsibilities:

a) Develop and deliver long-term strategic goals for data architecture vision and standards in conjunction with data users, department managers, clients, and other key stakeholders;
b) Participate in the creation and ongoing operation of the corporate data strategy and establish policies and procedures for sound data governance;
c) Conceptualize data products including dashboards and visualizations required to meet the organization's objectives;
d) Create short-term tactical solutions to achieve long-term objectives and an overall data management roadmap;
e) Establish processes for governing the identification, collection, and use of corporate metadata; take steps to assure metadata accuracy and validity;
f) Establish methods and procedures for tracking data quality, completeness, redundancy, and improvement;
g) Conduct data capacity planning, life cycle, duration, usage requirements, feasibility studies, and other tasks;
h) Create strategies and plans for data security, backup, disaster recovery, business continuity, and archiving;
i) Ensure that data strategies and architectures are in regulatory compliance; and
j) Assess and cultivate long-term strategic goals for database development in conjunction with end users, managers, clients, and other stakeholders.

Minimum Qualifications:

a) An undergraduate degree in a related field;
b) Certification related to business intelligence; and
c) Experience as a Business Intelligence / Data Warehouse (BI/DW) Specialist.

2. The following are the specific descriptions for each Role in Service Category #2 - Project Management:

Role #3 - Project Management Office Lead

Responsibilities:

a) Establish, implement, develop, and control best practices for IT project management throughout the organization;
b) Lead complex transformation programs and ensure each project stream/component is managed using appropriate processes, tools and disciplines;
c) Build, maintain and oversee the enterprise program management framework using 'agile' practices for driving program deliverables;
d) Oversee and maintain the overall program delivery schedule, integrating with individual work-stream schedules and clearly showing timeframes, resourcing, dependencies and critical paths;
e) Support subordinate Program Project Managers in overseeing the provision of all resources for the project (internal, vendor, other contractors, any other third party/seconded resources);

f) Support subordinate Program Project Managers in reviewing and maintaining all statements of work for all project activities; manage and report on all program financials, including forecasts, reporting actuals and explaining variances to budgets;
g) Support in preparing for and managing change associated with Modernization including change readiness assessment; collaboration with the Enterprise Risk Management (ERM) team; provide content to the Communications representatives;
h) Coordinate the governance process for transformation programs, preparing reporting for governing bodies; and
i) Develop and manage a program to periodically assess the quality of work and satisfaction with vendor and wider team performance, identifying issues and remedial actions, and coordinating actions to address issues.

Minimum Qualifications:

a) Post-secondary degree/diploma in a related field;
b) Project Management Professional (PMP) certification; and
c) Experience as an IT Project Manager

Role #4 - Project Manager

Responsibilities:

a) Lead the full project lifecycle from initiation to closure, including project planning, resource allocation, risk management, and quality assurance within previously agreed time, cost and performance parameters;
b) Define project objectives, scope, deliverables and budgetary requirements in collaboration with stakeholders, ensuring alignment with organizational goals;
c) Develop and maintain detailed project plans, visual diagrams, schedules, and budgets, and monitor progress against established milestones;
d) Conduct regular project status meetings, prepare progress reports, report progress of the project on an ongoing basis and at scheduled points in the life cycle;
e) Stay current with emerging technologies and project management tools, industry trends, and best practices in IT project management;
f) Coordinate and lead project teams, fostering a collaborative and high-performance work environment;
g) Facilitate effective communication and ensure stakeholders are informed about project status, risks, and changes; and
h) Support development of project management procedures and tools, evaluate project outcomes, conduct post-implementation reviews, and identify lessons learned for future projects.

Minimum Qualifications:

a) Post-secondary degree/diploma in a related field;
b) PMP or PRINCE2 certification;
c) Proven experience as an IT Project Manager, preferably in a government or public sector environment;
d) Strong knowledge of project management methodologies, tools, and techniques;
e) Solid understanding of software development lifecycle (SDLC) methodologies and experience working with agile frameworks (e.g., Scrum, Kanban);
f) Proficiency in project management software, collaboration tools, and Microsoft Office suite; and
g) Demonstrated ability to manage multiple projects simultaneously, prioritize tasks, and adapt to changing priorities.

Role #5 - Project Administrator / Coordinator

Responsibilities:

a) Assist project management and data processing professionals, technical users and end users in project coordination and synchronization tasks and administrative matters related to the project;
b) Provide administrative and technical support of a clerical nature as required to a project team;
c) Assist in performing such tasks as maintaining project documentation and application/system libraries;

d) Schedule project meetings and keep minutes;
e) Act as the first or single point of contact in a "hot-line" situation by accepting incoming calls, logging calls, attempting to resolve simple problems and following established procedures for more difficult problems;
f) Track project change requests;
g) Maintain and update relevant project information in manual and/or electronic files; project information might include such things as project activity schedule, status reports, correspondence and updating workflows;
h) Use computer tools, aids, system control languages on Personal Computers (PCs), minis, or mainframes to perform work;
i) Assist in the development of standardized project and communications tools; and
j) Prepare and distribute project materials.

Minimum Qualifications:

a) Post-secondary diploma/degree in a related field; and
b) Proficiency with Project Management tools e.g., MS Project, MS Excel, MS Planner etc.

3. The following are the specific descriptions for each Role in Service Category #3 - Cyber Security:

Role #6 - Security Analyst

Responsibilities:

a) Primary duty is the day-to-day operations of the in-place security solutions and the identification, investigation and resolution of security breaches detected/reported by the business;
b) Participate in the planning and design of enterprise security architecture, under the direction of the IT Security Manager, where appropriate;
c) Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures) under the direction of the IT Security Manager, where appropriate;
d) Participate in the planning and design of an enterprise Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), under the direction of the IT Security Manager, where appropriate;
e) Review logs and reports of all in-place devices, whether they be under direct control (i.e. security tools) or not (e.g. workstations, servers, network devices); interpret implications of that activity and devise plans for appropriate resolution;
f) Participate in investigations into problematic activity;
g) Participate in disaster recovery testing;
h) Develop and implements business and IT continuity/recovery strategies;
i) Provide advice and guidance to technical teams in the performance of their duties related to the ongoing design, development and implementation of continuity/security recovery capabilities in the areas of infrastructure (hardware, software, and networks), application development, and data management;
j) Develop Risk Management deliverables including Threat Risk Assessments (TRA), Statements of Sensitivity (SOS), Vulnerability Analysis (VA) and/or Security Gap Analysis evaluating Information Technology Safeguards (ITS) safeguards;
k) Define Recovery Objectives and Timeframes, including recovery times, expected losses, and priorities;
l) Research and document solutions for Intrusion Detection, Secure Networks, User Management and Control Systems, Information Protection Strategies, Recovery Requirements, and Information Technology Security Evaluation Criteria (ITSEC) challenges;
m) Prepare Cost/Benefit Analysis of ITSEC and Recovery Strategies and presents findings to Senior Management;
n) Conduct Threat Risk Assessments using qualitative and quantitative risk analysis methodologies such as annual loss expectancy, estimated annual cost, threat tree analysis, cause-sequence analysis, hazard and operability analysis, interface analysis and consultative, objective and bi-functional risk analysis;
o) Configure and manage enterprise firewalls, including the modification firewall rules, analyzing firewall log files and implementing corrective action;

p) Participate in the design and execution of vulnerability assessments, penetration tests, and security audits;
q) Perform the deployment, integration, and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically and CDIC's security documents specifically; and
r) Recommend additional security solutions or enhancements to existing security solutions to improve overall enterprise security.

Minimum Qualifications:

a) An undergraduate degree in a related field; and
b) Certified Information Systems Security Professional (CISSP), is an asset.

Role #7 - Application Security Administrator

Responsibilities:

a) Perform the development, configuration, testing, deployment and integration of application security;
b) Design, perform, and/or oversee penetration testing of all applications to identify system vulnerabilities;
c) Perform security reviews of applications through code implementation and review, application configuration and penetration testing;
d) Encryption of Transport Layer Security (TLS) in transit and database encryption at rest;
e) Design, implement, and report on security system and end user activity audits;
f) Design and implement Disaster Recovery Plan for operating systems, databases, networks, servers, and software applications;
g) Deploy, manage, and maintain all security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and antivirus software;
h) Monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity; interpret activity and make recommendations for resolution;
i) Recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach;
j) Assess need for any security reconfigurations (minor or significant) and execute them if required;
k) Interact and negotiate with vendors, outsourcers, and contractors to obtain protection services and products;
l) Recommend, schedule, and perform security improvements, upgrades, and/or purchases;
m) Manage and/or provide guidance to junior members of the team; and
n) Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices.

Minimum Qualifications:

a) An undergraduate degree in a related field;
b) Previous experience as a Security Analyst (range of experience years; 3-5 years); and
c) Knowledge of Open Web Application Security Project (OWASP), Secure Sockets Layer / Transport Layer Security (SSL/TLS) and Transmission Control Protocol / Internet Protocol (TCP/IP) protocols.

Role #8 - IT Security Architect

Responsibilities:

a) Assess and understand CDIC's current security architecture and posture and provide recommendations for improvement and risk reduction;
b) Work closely with IT, Application, and data architects to develop an architectural framework and guiding principles that will define and maintain our future enterprise architecture;
c) Plan and design an enterprise security architecture and document how the implementation of a new technology impacts the security posture of the current environment;
d) Provide subject matter expertise to senior management and technical teams, and support the design, deployment, configuration, and monitoring/evaluation of a secure hybrid environment (on

premises and cloud) in the areas of infrastructure (hardware, software, and networks), secure application development, and secure data management;
e) Define and communicate security requirements with business and technical teams for new corporate projects and business operations;
f) Perform security assessments, identify gaps, and provide recommendations to improve overall enterprise security and to ensure compliance with regulatory and security requirements;
g) Research and propose new solutions (including cost and effort estimates) for Cloud Security, Network Security, Perimeter Defense, Identity and Access Management, Vulnerability Management, Secure SDLC (Software Development Life Cycle), and other areas as required;
h) Perform planning, deployment, testing, and documentation of new security solutions or enhancements to existing security solutions in accordance with security best practices and CDIC's policies;
i) Participate in the design and execution of vulnerability assessments, penetration tests, security audits, and Threat Risk Assessments, providing recommendations on risk avoidance, mitigation, and issue resolution;
j) Implement recommendation actions and apply fixes to address gaps identified by assessments and compliance tools such as Azure/365 compliance centers, Microsoft Defender for Cloud and Qualys;
k) Identify and prioritize system functions required to promote continuous availability of critical business processes and assist in planning, developing, and testing enterprise Disaster Recovery and Business Continuity Plans;
l) Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures);
m) Provide input on security requirements to be included in requests for proposal (RFPs), statements of work (SOWs), and other procurement documents;
n) Whenever required, manage enterprise security systems including but not limited to firewalls, VPN (Virtual Private Networks), IPS/IDS (Intrusion Detection and Prevention Systems), Key Vaults, PKI (Public Key Infrastructure), EDR (Endpoint Detection and Response), Antimalware, Vulnerability Scanners, network Terminal Access Point (TAP), SIEM (Security Information Event Manager), and PIM (Privileged Identity Manager); and
o) Participate in investigations and troubleshooting of security-related issues, as required.

Minimum Qualifications:

a) An undergraduate or graduate degree in Information Technology or equivalent;
b) Certification in one or more of the following: CISSP, Certified Information Security Manager (CISM), Global Information Security Professional (GISP), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Auditor (CISA), The Open Group Architecture Framework (TOGAF), or Sherwood Applied Business Security Architecture (SABSA), Certified Cloud Security Professional (CCSP);
c) Strong knowledge of relevant industry standards such as ISO 27001, NIST, and ITSG-33;
d) Previous relevant experience in IT security architecture; and
e) Azure/O365 Cloud experience is an asset.

Role #9 - Ethical / White Hat Hacker (or Penetration Tester)

Responsibilities:

a) Primary duty includes conducting comprehensive assessments of computer systems, networks, web applications, and other digital assets to identify potential security vulnerabilities;
b) Model and/or Handle threats for applications, systems, infrastructure and concepts;
c) Plan and perform controlled attacks on systems and networks to exploit identified vulnerabilities in a controlled and ethical manner. This involves simulating real-world hacking techniques to assess the effectiveness of security measures and identify potential points of compromise.
d) Analyze components and configurations in finding out weak points;
e) Perform network security testing, web application security testing, wireless network security assessment, social engineering assessment, security audits, source code reviews and threat analysis;
f) Develop comprehensive and accurate reports and presentations for both technical and executive audiences;
g) Develop proposals for an appropriate counteraction and generate analysis and reports;
h) Provide recommendations to remediate identified gaps;

i) Present results to different committees;
j) Work closely with other cybersecurity professionals, system administrators, and developers to implement recommended security controls, patches, and fixes to mitigate identified vulnerabilities and enhance overall system security; and
k) Conduct workshops or live hackings at the customers location or in-house.

Minimum Qualification:

a) An undergraduate or graduate degree in Information Technology or equivalent;
b) Certification in one or more of the following: Certified Ethical Hacker (CEH), GIAC Penetration Tester (GPEN), Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), Certified Information Systems Security Professional (CISSP), Certified Penetration Testing Engineer (CPTE);
c) Relevant experience as a Penetration Tester and/or IT Security Analyst, Developer/Software Engineer, Network Administrator or Security Engineer; and
d) Azure/O365 Cloud experience, is an asset.

Role #10 - Azure Security Architect

Responsibilities:

a) Primary duty includes providing subject matter expertise and supporting the secure design, implementation and operation of our CDIC's Azure Cloud infrastructure;
b) Collaborate with stakeholders to develop and implement secure Azure cloud architecture and solutions. Ensure the integration of appropriate security controls and mechanisms, such as identity and access management, network security, data protection, encryption, and monitoring;
c) Establish and enforce Azure security governance frameworks, policies, and standards. Conduct regular security assessments and audits to identify vulnerabilities, risks, and compliance gaps. Develop and implement remediation strategies to address identified issues;
d) Define the organization's Azure security strategy and roadmap, aligned with business objectives and risk appetite. Stay updated with the latest Azure security features, tools, and technologies to drive continuous improvement and innovation in security architecture;
e) Conduct threat modeling exercises and risk assessments to identify and prioritize potential threats and vulnerabilities. Collaborate with other security teams to develop mitigation strategies and recommend security controls to address identified risks;
f) Lead the design and review of Azure cloud infrastructure components, including virtual networks, storage accounts, virtual machines, and Azure services. Ensure adherence to security best practices, industry standards, and regulatory requirements;
g) Collaborate with incident response teams to develop and enhance Azure cloud-specific incident response plans and playbooks. Participate in security incident investigations, provide expertise on Azure-specific incidents, and contribute to post-incident reviews and lessons learned;
h) Promote a security-conscious culture within the organization. Develop and deliver training programs to educate stakeholders on Azure security best practices, secure coding, and compliance requirements; and
i) Work closely with cross-functional teams, including cloud architects, developers, operations teams, and compliance officers, to ensure security is integrated throughout the Azure cloud lifecycle. Communicate security risks, recommendations, and requirements to technical and non-technical stakeholders in a clear and concise manner.

Minimum Qualifications:

a) An undergraduate or graduate degree in Information Technology or equivalent;
b) Microsoft Certified: Azure Security Engineer Associate or equivalent Microsoft Certification;
c) In-depth understanding of network security, identity and access management, encryption, and data protection mechanisms;
d) Experience implementing secure Azure cloud architectures;
e) Experience applying Information Technology Security Guidance (ITSG-33) and Government of Canada security standards in a Cloud environment; and
f) Certified Information Systems Security Professional (CISSP) and Certified Cloud Security Professional (CCSP), or similar certifications are considered an asset.

Role #11 - Azure Security Administrator

Responsibilities:

a) Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices;
b) Participate in the design, implementation and testing of disaster recovery plans for systems, databases, networks, servers, and software applications;
c) Assess need for any security reconfigurations (minor or significant) and execute them if required;
d) Keep current with emerging security alerts and issues;
e) Conduct research on emerging products, services, protocols, and standards in support of security enhancement and development efforts;
f) Recommend, schedule, and perform security improvements, upgrades, and/or purchases;
g) Manage enterprise security systems including but not limited to firewalls, VPN (Virtual Private Networks), IPS/IDS (Intrusion Detection and Prevention Systems), Key Vaults, PKI (Public Key Infrastructure), EDR (Endpoint Detect and Response) (Endpoint Detection and Response), Antimalware, Vulnerability Scanners, network Terminal Access Point (TAP), SIEM (Security Information Event Manager), PIM (Privileged Identity Manager);
h) Administer and maintain end user accounts, permissions, and access rights;
i) Manage Onboarding and Offboarding activities for staff and consultants;
j) Manage connection security for local area networks, the company web site, the intranet, and e-mail communications;
k) Design, perform, and/or oversee penetration testing of all systems to identify system vulnerabilities;
l) Design, implement, and report on security system and end user activity audits;
m) Monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interpret activity and make recommendations for resolution;
n) Recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach;
o) Perform system backups;
p) Manage and/or provide guidance to junior members of the team;
q) Process Service requests and respond to incidents.;
r) Whenever required, participate in investigations and troubleshooting security related issues; and
s) Perform other related duties as required.

Minimum Qualifications:

a) Certification in one or more of the following: CISSP (Certified Information Systems Security Professional); CEH (Certified Ethical Hacker); CCSE (Check Point Certified Expert); CCSP (Certified Cloud Security Professional); Azure Security Engineer Associate; Microsoft 365 Security Administrator Associate; GWEB (GIAC Web Application Defender); CSSLP (Certified Secure Software Lifecycle Professional);
b) Experience applying ITSG-33 and government security standards in a Cloud environment; and
c) Experience managing secure Azure Cloud Environments.

Role #12 – Cyber Forensics Specialist

Responsibilities:

a) Conduct deep security analysis on Windows and Unix computer systems;
b) Conduct deep security assessments in cloud environments, especially Azure;
c) Complete imaging systems under investigation in the cloud for investigations;
d) Manage full control of evidence life cycle;
e) Develop policy and technical procedures;
f) Forensic imaging and collection of electronic data;
g) Initial review and culling of data for E-Discovery matters;
h) Analysis of digital media and subsequent reporting of findings;
i) Data recovery;
j) Assist in investigations with information technology (“IT”) components;
k) Securing of digital evidence with the use of disk imaging techniques and preserving chain of custody;
l) Recovery and analysis of digital evidence;

m) Configure, test and maintain forensic support tools in a forensic laboratory environment;
n) Provide advice to team members and clients on proper data recovery steps and procedures;
o) Develop links within the organization that can contribute to thought leadership;
p) Build and maintain excellent relationships with existing and target client organizations;
q) Develop excellent relationships with colleagues in other areas of the organization; and
r) Document, report and present findings to Senior Management.

Minimum Qualifications:

a) Experience practicing computer/digital forensic investigations, eDiscovery, investigation and support work (range of experience years; 2-5 years); and
b) Certification in one or more of the following; CISSP (Certified Information Systems Security Professional); CCE (Certified Computer Examiner); CFCE (Certified Forensic Computer Examiner); CHFI (Computer Hacking Forensic Investigator); GCFA (GIAC Forensic Analyst).

Role #13 – Security Engineer (Application/Network)

Responsibilities:

a) Provide subject matter expertise to senior management and technical teams, and support the design, deployment, configuration, and monitoring/evaluation of a secure hybrid environment (on premises and Cloud) in the areas of infrastructure (hardware, software, and networks), secure application development, and secure data management;
b) Define and communicate security requirements with business and technical teams for new corporate projects and business operations;
c) Perform security assessments, identify gaps, and provide recommendations to improve overall enterprise security and to ensure compliance with regulatory and security requirements;
d) Research and propose new solutions (including cost and effort estimates) for Cloud Security, Network Security, Perimeter Defense, Identity and Access Management, Vulnerability Management, Secure SDLC (Software Development Life Cycle), and other areas as required;
e) Perform planning, deployment, testing, and documentation of new security solutions or enhancements to existing security solutions in accordance with security best practices and CDIC's policies;
f) Participate in the design and execution of vulnerability assessments, penetration tests, security audits, and Threat Risk Assessments, providing recommendations on risk avoidance, mitigation, and issue resolution;
g) Implement recommendation actions and apply fixes to address gaps identified by assessments and compliance tools such as Azure/365 compliance centers, Microsoft Defender for Cloud and Qualys;
h) Participate in the planning and design of enterprise security architecture and document how the implementation of modern technology impacts the security posture of the current environment;
i) Identify and prioritize system functions required to promote continuous availability of critical business processes and assist in planning, developing, and testing enterprise Disaster Recovery and Business Continuity Plans;
j) Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures);
k) Manage enterprise security systems including but not limited to firewalls, VPN (Virtual Private Networks), IPS/IDS (Intrusion Detection and Prevention Systems), Key Vaults, PKI (Public Key Infrastructure), EDR (Endpoint Detect and Response) (Endpoint Detection and Response), Antimalware, Vulnerability Scanners, network Terminal Access Point (TAP), SIEM (Security Information Event Manager), PIM (Privileged Identity Manager), as required;
l) Participate in investigations and troubleshooting security related issues, as required; and
m) Perform other related duties as required.

Minimum Qualifications:

a) An undergraduate or graduate degree in Information Technology or equivalent; and
b) Certification in one or more of the following: CISSP (Certified Information Systems Security Professional); CEH (Certified Ethical Hacker); CCSE (Check Point Certified Expert); CCSP (Certified Cloud Security Professional); Azure Security Engineer Associate; Microsoft 365 Security

Administrator Associate; GWEB (GIAC Web Application Defender); CSSLP (Certified Secure Software Lifecycle Professional).

Role #14 – SOC Analyst

Responsibilities:

a) Provide response and actions needed for security events including but not limited to intrusion detection, malware infections, denial of service attacks, privileged account misuse and network intrusions;
b) Follow defined workflow and processes for threat remediation and escalation/handoff where required;
c) Utilize a variety of cloud-based and on-premises security tools and techniques to proactively analyze suspicious events, network anomalies and other potential threats to determine validity, impact, scope and recovery options;
d) Use automated malware analysis tools to determine threat impact and taking actions appropriately;
e) Support and administration of security tools and platforms in diverse, cloud-based and on-premises environments;
f) Configure and monitor Security Information and Event Management (SIEM) platform for security alerts. Integrate and work with the firm's Managed Security Services Provider (MSSP) services staff to guide and manage decisions related to alerts;
g) Improve the service level for security operations and monitoring. Create and maintain system documentation for security event processing. Expand the usage of security monitoring tools to improve the security of the environment based on business use cases or changes in threat landscape, root causes from security incident response, or output from security analytics;
h) Perform duties related to installing MFA (Multi Factor Authentication) on users' machines and helping users with general onboarding;
i) Perform software installation as needed on user machines for security related software;
j) Guide new employees and contractor onboarding process by working with individuals to setup access and follow prescribed procedures; and
k) Help develop run books and document technical security procedures.

Minimum Qualifications:

a) Four (4) or more years of relevant work experience;
b) An undergraduate degree in Computer Science, Computer/Data Systems Management or a related field or discipline, and/or equivalent experience;
c) Experience in an Operations Center (SOC/NOC) / monitoring environment;
d) Experience working with SIEM technologies (e.g., ArcSight, QRadar, Splunk, Azure Sentinel, etc.) or Managed Security Service Providers (MSSP); and
e) GIAC Security Certification such as GSEC, GMON, GISP, or ISC2 CISSP OSCP, GIAC GISP, or GIAC GCIH are preferred.

Role #15 – SOC Lead/Manager

Responsibilities:

a) Manage the SIEM operations and develop processes, procedures and run books;
b) Triage, assess and manage alerts and incidents;
c) Manage security incident handling and response operations from end to end, especially L3 and L4 or critical and high incidents in collaboration and through direction from Manager, Cyber Security Operations;
d) Manage the Service tickets (Change, Incidents, Service requests, and problem tickets) and assign based on volume and workload to team members;
e) Develop use cases in MS Sentinel through continuous development and improvements;
f) Review and evaluate daily threat feeds;
g) Manage vulnerability scanning, analysis and dissemination of vulnerabilities and remediation to SMEs to address identified risks;
h) Manage threat feeds and threat briefings coming from multiple sources to ensure vigilance especially related to critical and high issues uncovered in the technology space;
i) Perform a hands-on investigation as required on systems, applications, networks, Cloud environments etc.;

j) Assist to protect IT hardware, software and data against modification, destruction, and accidental or unauthorized disclosure;
k) Assist in authentication and access control by designing, administering and controlling proven security systems;
l) Analyze IT system vulnerabilities and implement protective measures to back up, restore and secure systems;
m) Lead development projects and complex, highly innovative strategic initiatives, such as the development of IT security standards and policies;
n) Recommend planning and execution of operationally and conceptually complex projects and initiatives that require comprehensive analysis and understanding of the organization and line of business;
o) Coordinate and interact with stakeholders;
p) Act as a SME resource person and coach for decision-making bodies;
q) Assist with managing encryption processes such as PGP key management and creation, GOC My key, Entrust SSL certificate management, etc.;
r) Lead vulnerability management by conducting scans and completing analysis and communication with SMEs on resolutions and vulnerability tracking; and
s) Other security operations duties as assigned.

Minimum Qualifications:

a) An undergraduate degree or graduate degree in a related field, or equivalent;
b) A minimum of six (6) years of relevant experience; and
c) Certifications in one or more of security certifications. GIAC GMON, GIAC GCIH or Other Incident handling and Response, CISSP, CISA, CEH, OSCP, or any other technical certification is an asset.

Role #16 – Cloud Security Specialist

Responsibilities:

a) Develop security strategy plans and roadmaps based on sound enterprise architecture practices;
b) Develop and maintain security architecture artifacts (e.g., models, templates, standards and procedures) that can be used to leverage security capabilities in projects and operations;
c) Determine baseline security configuration standards for operating systems, network segmentation and identity and access management (IAM);
d) Develop standards and practices for data encryption and tokenization in the organization, based on the organization's data classification criteria;
e) Draft security procedures and standards to be reviewed and approved by executive management;
f) Track developments and changes in the digital business and threat environments to ensure that they're adequately addressed in security strategy plans and architecture artifacts;
g) Validate IT infrastructure and other reference architectures for security best practices and recommend changes to enhance security and reduce risks, where applicable;
h) Validate security configurations and access to security infrastructure and application tools, including firewalls, IPSs, WAFs, Keyvaults, Vulnerability Scanners, SIEMs and anti-malware/endpoint protection systems;
i) Conduct or facilitate threat modeling of services and applications that tie to the risk and data associated with the service or application;
j) Ensure a complete, accurate and valid inventory of all systems, infrastructure and applications that should be logged by the security information and event management (SIEM) or log management tool;
k) Coordinate with relevant teams to advocate secure coding practices;
l) Coordinate with the privacy officer or office to document data flows of sensitive information in the organization (e.g., PII) and recommend controls to ensure that this data is adequately secured (e.g., encryption and tokenization);
m) Review network segmentation to ensure least privilege for network access;
n) Participate in application and infrastructure projects to provide security-planning advice;
o) Liaise with the internal audit (IA) team to review and evaluate the design and operational effectiveness of security-related controls;
p) Responsible for End-to-End security maintenance and security testing of cloud infrastructure;
q) Recommend and implement new services to enhance the security of CDIC's cloud environment based on best practices and guidance from the GOC standards;

r) Manage enterprise security systems including but not limited to firewalls, VPN (Virtual Private Networks), IPS/IDS (Intrusion Detection and Prevention Systems), Key Vaults, PKI (Public Key Infrastructure), EDR (Endpoint Detect and Response) (Endpoint Detection and Response), Antimalware, Vulnerability Scanners, network Terminal Access Point (TAP), SIEM (Security Information Event Manager), PIM (Privileged Identity Manager), as required;
s) Whenever required, participate in investigations and troubleshooting security related issues; and
t) Perform other related duties as required.

Minimum Qualifications:

a) An undergraduate or graduate degree in Information Technology or equivalent; and
b) Certification in one or more of the following: CISSP (Certified Information Systems Security Professional); CEH (Certified Ethical Hacker); CCSE (Check Point Certified Expert); CCSP (Certified Cloud Security Professional); Azure Security Engineer Associate; Microsoft 365 Security Administrator Associate; GWEB (GIAC Web Application Defender); CSSLP (Certified Secure Software Lifecycle Professional), Certified Cloud Security Professional CCSP (Certified Cloud Security Professional).

Role #17 – Security Administrator

Responsibilities:

a) Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices;
b) Participate in the design, implementation and testing of disaster recovery plans for systems, databases, networks, servers, and software applications;
c) Assess need for any security reconfigurations (minor or significant) and execute them if required.
d) Keep current with emerging security alerts and issues;
e) Conduct research on emerging products, services, protocols, and standards in support of security enhancement and development efforts;
f) Recommend, schedule, and perform security improvements, upgrades, and/or purchases;
g) Manage enterprise security systems including but not limited to firewalls, VPN (Virtual Private Networks), IPS/IDS (Intrusion Detection and Prevention Systems), Key Vaults, PKI (Public Key Infrastructure), EDR (Endpoint Detect and Response) (Endpoint Detection and Response), Antimalware, Vulnerability Scanners, network Terminal Access Point (TAP), SIEM (Security Information Event Manager), PIM (Privileged Identity Manager);
h) Administer and maintain end user accounts, permissions, and access rights;
i) Manage Onboarding and Offboarding activities for staff and consultants;
j) Manage connection security for local area networks, the company web site, the intranet, and e-mail communications;
k) Design, perform, and/or oversee penetration testing of all systems to identify system vulnerabilities;
l) Design, implement, and report on security system and end user activity audits;
m) Monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interpret activity and make recommendations for resolution;
n) Recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach;
o) Perform system backups;
p) Manage and/or provide guidance to junior members of the team;
q) Process Service requests and respond to incidents;
r) Whenever required, participate in investigations and troubleshooting security related issues; and
s) Perform other related duties as required.

Minimum Qualifications:

a) Post-secondary diploma/degree in the field of computer science and/or seven (7) years equivalent work experience; and
b) Certification in one or more of the following: CISSP (Certified Information Systems Security Professional); CEH (Certified Ethical Hacker); CCSE (Check Point Certified Expert); CCSP (Certified Cloud Security Professional); Azure Security Engineer Associate; Microsoft 365 Security Administrator Associate; GWEB (GIAC Web Application Defender); CSSLP (Certified Secure

Software Lifecycle Professional), Certified Cloud Security Professional CCSP (Certified Cloud Security Professional).

Role #18 – Governance Risk and Compliance (GRC) Analyst

Responsibilities:

a) Help define and lead the implementation of an enterprise-wide strategy focused on the reduction of technology risk;
b) Develop and maintain a Cyber Risk register including critical assets, vulnerabilities and threats;
c) Perform threat modeling exercises on a regular and ad-hoc basis to identify existing and new emerging threats relevant to CDIC;
d) Develop and maintain Cyber policies, standards, procedures, and guidelines;
e) Develop cyber communication plans and content on security awareness and best practices;
f) Work with IT, business and internal and external audit teams to perform security and compliance assessments on new and existing systems, processes, and technologies;
g) Participate in disaster recovery and business continuity planning and testing;
h) Lead efforts to achieve compliance with various frameworks and regulations by consulting and working with the relevant IT and business staff and control owners;
i) Perform periodic gap assessments to validate compliance on an ongoing basis to ensure that proper controls are in place and risks are appropriately mitigated; and
j) Conduct Government of Canada Security Assessments as an assessor using the SA&A process and drafting Security Assessments Reports outlining the critical risks and recommending remediation to senior Management.

Minimum Qualifications:

a) An undergraduate degree in Information Systems, Cybersecurity, or a related field and/or five (5) years equivalent work experience;
b) Three (3) years of relevant experience in the IT risk, security, compliance or audit field; and
c) Certification in one or more of the following: CISSP (Certified Information Systems Security Professional); CISA (Certified Information Systems Auditor); CRISC (Certified in Risk and Information Systems Control); OCEG GRCP (GRC Professional Certification); OCEG GRCA (GRC Auditor Certification); ISO/IEC 27001 Lead Implementer; ISO/IEC 27001 Lead Auditor.

4. The following are the specific descriptions for each Role in Service Category #4 - Enterprise Technology:

Role #19 - Storage Administrator / Virtualization Architect

Responsibilities:

a) Perform operation and performance tuning of storage platforms across CDIC to ensure high levels of data quality, availability and security;
b) Perform tasks necessary to fulfill Service Level Agreements (SLA's) with end-users regarding storage allocations, limitations, security and availability;
c) Perform/test backups and restores to ensure that enterprise data is effectively protected;
d) Anticipate, mitigate, identify, respond to, and resolve issues with storage devices, storage access, and data retrieval;
e) Research and make recommendations on storage products, services, and standards in support of procurement/development efforts;
f) Monitor, analyze, and predict trends for storage equipment performance, space allocation, and data growth to recommend enhancements to the IT storage team;
g) Develop routines for end-users to facilitate storage best practices, including desktop storage administration;
h) Perform storage server/database transaction and security audits leading to identification and mitigation of security threats to enterprise data; recommend and implement changes where necessary;
i) Work with systems and Database Administrators to implement storage architectures that utilize best practices;

j) Implement redundant systems, policies, and procedures for disaster recovery and archiving to ensure effective protection and integrity of storage appliances and stored data assets;
k) Participate in and support capacity planning and development of long-term strategic goals for CDIC's storage in conjunction with data owners and department managers; and
l) Participate in the planning and implementation of policies and procedures to ensure storage provisioning, efficiency and maintenance that is consistent with CDIC's goals, industry best practices and regulatory requirements.

Minimum Qualifications:

a) An undergraduate degree in Cyber Security, Information Systems, Information Technology, Computer Science or related field and/or related technical diploma; and
b) Previous relevant experience in Storage Architecture.

Role #20 - Systems Architect (Network, Data, Applications)

Responsibilities:

a) Develop technical architectures, frameworks and strategies, either for an organization or for a major application area, to meet the business and application requirements;
b) Analyze and evaluate alternative technology solutions to meet business problems;
c) Ensure the integration of all aspects of technology solutions;
d) Analyze functional requirements to identify information, procedures and decision flows;
e) Evaluate existing procedures and methods; identify and document database content, structure, and application sub-systems, and develop data dictionary;
f) Define and document interfaces of manual to automated operations within application sub-systems, to external systems and between new and existing systems;
g) Define input/output sources, including detailed plan for technical design phase, and obtain approval of the system proposal;
h) Model business and systems processes based on findings through use case scenarios, workflow diagrams, and data models;
i) Develop and execute test plans to check infrastructure and systems technical performance; report on findings and make recommendations for improvement;
j) Develop and manage a systems capacity plan;
k) Provide guidance to junior members of the team;
l) Identify the policies and requirements that drive out a particular solution;
m) Monitor industry trends to ensure that solutions fit with government and industry directions for technology;
n) Identify and document system specific standards relating to programming, documentation and testing, covering program libraries, data dictionaries, naming conventions, etc.;
o) Design and implement long-term strategic goals and short-term tactical plans for managing and maintaining corporate systems and software;
p) Ensure that proposed and existing systems architectures are aligned with organizational goals and objectives;
q) Provide architectural expertise, direction, and assistance to Systems Analysts, Systems Engineers, other Systems Architects, and software development teams; and
r) Review new and existing systems design projects and procurement or outsourcing plans for compliance with standards and architectural plans.

Minimum Qualifications:

a) An undergraduate degree in a related field; and
b) Previous relevant experience as a Systems Architect.

Role #21 – Azure Architect

Responsibilities:

a) Provide subject matter expertise in Cloud Architecture and supports the design, deployment, configuration and monitoring/evaluation of Azure infrastructure, networking, applications, data platform and solution administration; conducts analysis and provides expert support to the planning and conduct of migration projects.

Minimum Qualifications:

a) Post-secondary diploma/degree in Computer Science, Computer Engineering, Information Technology or equivalent; and
b) Microsoft Certified: Azure Solutions Architect Expert or equivalent Microsoft Certification.

Role #22 - Azure Administrator

Responsibilities:

a) Support system design and implementation, including install/creation, configuration, deployment, monitoring/maintenance and evaluation, focusing on compute, storage, networking, security, and integration aspects, including user administration.

Minimum Qualifications:

a) Microsoft Certified Azure Administrator Associate or equivalent Microsoft Certification; and
b) Previous relevant experience in the role.

Role #23 - Azure Data Base Administrator

Responsibilities:

a) Support the design and implementation of database solutions for Structured Query Language (SQL) Server and MS Azure, including database security, availability, performance, scalability and recovery requirements.

Minimum Qualifications:

a) Post-secondary diploma/degree in Computer Science, Computer Engineering, Information Technology or equivalent;
b) Microsoft Certified Solutions Associate (MCSA) SQL 2016 (any), Microsoft Certified Technology Specialist, Microsoft Certified IT Professional, Microsoft Certified Azure Database Associate or equivalent Microsoft Certification; and
c) Hands on technical experience with SQL Server.

Role #24 - Webmaster

Responsibilities:

a) Coordination, planning, maintenance and accessibility of web site content while ensuring the consistency of the web site's look and feel;
b) Create web pages including graphics and general web site design;
c) Find, diagnose, and fix web site problems, including broken links (both internal and external), typographical errors, and formatting inconsistencies;
d) Develop and implement usability tests, analyze results and modify design accordingly;
e) Develop flowcharts (web site flow maps) depicting navigation and basic content;
f) Develop line drawings or block diagrams illustrating the priority of information, links, navigation, and space requirements;
g) Develop content diagrams showing the interactive connection between web pages;
h) Develop interactive prototypes showing basic form and functionality for both usability testing and presentations;
i) Prepare a long-term plan for web site development and presence, including standards and guidelines for content, based on business goals and input from stakeholders; and
j) Manage the acquisition and ongoing maintenance of the organization's domain names with the appropriate registrars.

Minimum Qualifications:
a) Post-secondary diploma/degree in a related field; and b) Previous relevant experience as a Webmaster.

5. The following are the specific descriptions for each Role in Service Category #5 - Technical Support:

Role #25 - Application Support Specialist
Responsibilities:
a) Installation, maintenance and troubleshooting of desktop computers, laptops and printer hardware and associated software as well as providing remote support for external desktop computer and laptop connections, wireless, and broadband; b) Provide problem recognition, isolation, research, resolution and follow-up; c) Provide 2nd level technical support; d) Provide systems administration duties such as creating and maintaining network accounts, performing basic security back-ups; e) Escalate more complex problems to senior support personnel to expedite resolution; f) Assist with the automation of desktop computer build processes and packaging applications; g) Troubleshoot and resolve network problems; h) Create problem and resolution logs for help desk activities; i) Ensure technical support issues are resolved in a prompt and efficient manner; j) Conduct basic development support services such as patch development and other related application support services; k) Plan or participate in the implementation of organization wide system upgrades, occasional project work, asset management, technical documentation and making recommendations on technology; l) Create and deploy feedback mechanisms for end users; analyzing results, making recommendations for support process improvements, and implementing changes; m) Resolve advanced application support issues; n) Coordinate emerging technology application specifications; o) Conduct research into software application products and services in support of development and purchasing efforts; p) Solve complex end-user technical problems that more junior levels cannot resolve; q) Serve as a user support liaison between vendors, information systems technicians, and end-user organizations; r) Provide training expertise and direction in the area of emerging technology and special application support; s) Emulate or reproduce technical problems encountered by users; t) Provide advice and training to users in response to identified difficulties; u) Recommend and implement complex security requirements; v) Provide business systems, network and Internet support to users in response to identified difficulties; and w) Collect, organize and maintain a problems and solutions log for use by others.
Minimum Qualifications:
a) Post-secondary certificate/diploma/degree in Computer Science or other relevant field from a recognized post-secondary institution; and b) Previous relevant experience as an Application Support Specialist.

Role #26 - Deskside Technical Support Analyst
Responsibilities:
a) Provide basic technical support / assistance to organization personnel for its standard desktop software suite, as well as printers and other peripherals; and b) Provide support for mobile devices, including related apps / software and peripherals.

Minimum Qualifications:

a) Post-secondary diploma/degree in a related field; and
b) Previous relevant experience as a Technical Support Analyst.

Role #27 - Service Desk Analyst

Responsibilities:

a) Perform a variety of network problem analysis and monitoring tasks, monitor network management systems and respond appropriately to user requests and problems;
b) Perform initial problem analysis and triage problems to other appropriate staff when appropriate;
c) Maintain liaison with network users and technical staff to communicate the status of problem resolution to network users; log and track requests for assistance;
d) Participate in on-site installations of network systems for users;
e) Perform other related duties incidental to the work described herein; and
f) Develop, implement, and/or participate in the distribution of network related information to users to include information such as help desk procedures and network handbooks.

Minimum Qualifications:

a) Post-secondary degree/diploma in a related field; and
b) Previous relevant experience as a Service Desk Analyst.

Role #28 - IT Service Management Specialist

Responsibilities:

a) Create and implement processes and procedures following Information Technology Service Management (ITSM) Best Practices;
b) Review and evaluate existing processes and procedures following ITSM Best Practices;
c) Provide guidance to CDIC staff in applying ITSM Best Practices;
d) Provide knowledge transfer to CDIC employees;
e) Develop, implement, and/or participate in the preparation of procedure manuals and documentation for help desk use;
f) Conduct periodic user satisfaction surveys and track user problem trends; make recommendations for improvements to the network systems and create reports based on information provided from user surveys and trends;
g) Record, monitor and report on service desk performance; and
h) Participate in the development of a comprehensive training plan for help desk procedures; assist in training personnel providing backup coverage.

Minimum Qualifications:

a) An undergraduate degree in a related field; and
b) Previous relevant experience as an ITSM Specialist, consulting on, developing, implementing and applying IT Service Management principles and processing.

Role #29 - Infrastructure Operations and Support

Responsibilities:

a) Test network performance and provide network performance statistics and reports; develop strategies for maintaining network infrastructure;
b) Consolidation of parallel networks onto a shared public or private infrastructure and integrating networks of recently merged or acquired enterprises into the original enterprise's network system;
c) Provide technical planning and support for a medium complexity network in a single location with some Virtual Private Network (VPN) connectivity;
d) Provide technical planning and support for high-end core Local Area Network (LAN) Switching products, including layer-3 switching;
e) Support a production TCP/IP wide-area network;
f) Provide Open Shortest Path First (OSPF), point-to-point and multipoint designs;
g) Develop and maintains Network system documentation;
h) Perform network troubleshooting;

i) Review coding and error detection methodologies;
j) Collect and preserve evidence to be admissible in court if needed;
k) Support the development of business cases;
l) Provide input into network modeling and simulation exercises;
m) Interpret the needs of applications and users into logical designs, SLAs and network management practices;
n) Write technical specifications, acceptance criteria, and perform evaluation of technical proposals for network related RFPs in a public sector environment;
o) Assess the impact of new applications and application changes in the Network;
p) Lead technical teams in specific Network improvement and upgrade projects.
q) Provide TCP/IP Network Management;
r) Review communications over local and wide area networks as to their ability to support data processing requirements;
s) Recommend changes to transmission networks, both in terms of hardware devices and switching points required to improve network performance;
t) Participate in the analysis, design, and implementation of communication networks for data processing transmissions requirements;
u) Support and manage storage, including Storage Area Network (SAN) and Network-Attached Storage (NAS) types;
v) Design and recommend short and long-term strategic plans to ensure infrastructure capacity meets existing and future requirements;
w) Review cabling standards and building designs;
x) Provide networking solutions to all server platforms;
y) Research, test and recommend the adoption of new technologies, hardware, and software and network protocols to enhance data processing requirements;
z) Recommend and coordinate the removal of outdated technologies, software and network protocols while maintaining or enhancing existing data processing requirements;
aa) Analyze, make recommendations for, and implement various virtualization projects / initiatives;
bb) responsible for providing technical support for on premises and Cloud (Azure and O365) technology; and
cc) Support operations for disaster recovery to ensure the effective backup and recovery of CDIC data.

Minimum Qualifications:

a) Post-secondary degree/diploma in a related field such as Computer Technology, Networking, Computer Science, or related field; and
b) Previous relevant experience as an Infrastructure Operations and Support Specialist.

Role #30 - Technical Writer / Trainer / Courseware Author (developer)

Responsibilities:

a) Document help text, user manuals, technical documentation, web page content, etc.;
b) Gather information concerning the features and functions provided by Developers;
c) Develop a table of contents for each document/manual and write or edit the required content;
d) Investigate the accuracy of the information collected by making direct use of the material being documented;
e) Prepare or coordinate the preparation of any required illustrations and diagrams;
f) Design the layout of documents / manuals;
g) Use word-processing, desktop publishing and graphics software packages to produce final camera-ready copy;
h) Review documentation standards and the existing project documentation;
i) Determine documentation requirements and make plans for meeting them;
j) Assess the audience for the documents/manuals which are required and prepare a statement of purpose and scope for each;
k) Perform needs assessment/analysis for training purposes;
l) Plan and monitor training projects;
m) Perform job, task, and/or content analysis;
n) Write criterion-referenced, performance-based objectives;
o) Recommend instructional media and strategies;
p) Develop performance measurement standards;

q) Develop training materials;
r) Prepare end-users for implementation of courseware materials;
s) Communicate effectively by visual, oral, and written form with individuals, small group, and in front of large audiences; and
t) Develop and deliver IT-related training material to small and medium-sized groups (5 to 50).

Minimum Qualifications:

a) Post-secondary degree/diploma in a related field; and
b) Previous relevant experience as a Technical Writer.

6. The following are the specific descriptions for each Role in Service Category #6 - SharePoint Support:

Role #31 - SharePoint Online Administrator

Responsibilities:

a) Administration of collaboration tools in support of CDIC's SharePoint tenants;
b) Oversee activity pertaining to the maintenance of SharePoint including incident and request tickets;
c) Responsible for maintaining end user access permissions and related system guidelines;
d) Provide defect and issue resolution to end users;
e) Establish access and control guidelines, maintain and monitor related infrastructure and develop standards for use of systems;
f) Recommend, schedule, and perform software and hardware improvements, upgrades, patches, reconfigurations, and/or purchases;
g) Coordinate with product vendors and/or service providers to resolve technical issues; and
h) Participate in and support capacity planning and the development of long-term strategic goals for SharePoint in conjunction with end-users and department managers.

Minimum Qualifications:

a) Post-secondary diploma/degree in Computer Science, Computer Engineering, Information Technology or equivalent; and
b) Previous relevant experience in the role.

Role #32 - SharePoint Online Architect

Responsibilities:

a) Lead the SharePoint team in the analysis, design development and deployment of SharePoint solutions;
b) Primary architect for all custom SharePoint solutions; lead complete software development life cycle, including design, analysis, configuring, programming and testing;
c) Educate developers on best practices for developing custom SharePoint solutions;
d) Provide expertise and support to business managers and other members of IT to determine how to best implement, support, and use SharePoint solutions;
e) Participate in SharePoint infrastructure projects;
f) Determine when SharePoint is not the right solution for a business problem and communicate this effectively to business leaders; and
g) Conduct research on emerging SharePoint development tools and strategies.

Minimum Qualifications:

a) Post-secondary diploma/degree in Computer Science, Computer Engineering, Information Technology or equivalent;
b) Previous relevant experience with SharePoint Architecture;
c) Previous relevant experience in SharePoint development creating solutions (apps, page layouts, workflows etc.); and
d) Experience with design, development or enterprise level portals.

Role #33 - SharePoint Online Developer
Responsibilities:
a) Design and develop portal content and applications that integrate with other enterprise systems and third-party products; b) Integrate non-SharePoint related services into SharePoint applications as needed; c) Assist other Developers, Analysts, and Designers in conceptualizing and developing SharePoint solutions; d) Provide expertise and support to end users and other members of the IT support team; e) Conduct research on emerging SharePoint development tools and strategies; and f) Recommend, schedule, and perform software improvements and upgrades.
Minimum Qualifications:
a) Post-secondary diploma/degree in the field of Computer Science or Software Engineering, and/or other relevant degree; b) Experience developing web applications using Microsoft and compatible technologies including SharePoint 2007/2010/2013, Visual Studio, VB.Net, and C#; c) Experience in .Net; and d) Experience with SharePoint.

7. The following are the specific descriptions for each Role in Service Category #7 - Alteryx Support:

Role #34 - Alteryx Developer
Responsibilities:
a) Design, develop, and maintain high performance Alteryx workflows for data transformation, data cleaning, data blending, and data analysis, processing high volumes of data.
Minimum Qualifications:
a) Post-secondary certificate/diploma/degree in a field of study related to data analysis (e.g. Information Systems, Computer Science, Data Science), or a related field; b) Previous relevant experience in the field of Business Intelligence and Analytics; c) Three (3) years of experience designing and developing/configuring workflows in Alteryx Designer and Alteryx Server; d) Experience with SQL; e) Experience with architecting high-performance solutions using relational databases; f) Experience in incremental/iterative (“agile-like”) development and configuration for data solutions; g) Expertise in development and configuration using Alteryx Designer and Alteryx Server; h) Strong problem-solving and analytical skills; and i) Excellent communication skills to effectively collaborate with team members and stakeholders.

8. The following are the specific descriptions for each Role in Service Category #8 - Application Development:

Role #35- Solution Architect
Responsibilities:
a) Support the design, deployment, configuration and monitoring/evaluation of infrastructure, networking, applications, data platform and solution administration; b) Document and develop in-depth knowledge of CDIC’s existing architecture; c) Assist with the design, development and implementation of systems; d) Manage the schedule of reviews that need to take place for projects that are in progress; e) Provide guidance to the junior staff in the early planning stage around the different solution patterns that may be appropriate for the specific solution; f) Inform stakeholders of solution architecture review outcomes;

g) Ensure that the IS, Data, and IT Architecture interests are considered and engagement with the respective architects occurs for all solutions;
h) Ensure that all individual solution architecture artifacts and changes are documented as per process standards and stored in the corporation's IA Library to facilitate compliance, organization, and access;
i) Manage and continuously improve the design and implementation of solution architecture processes and artifacts;
j) Provide subject matter expertise in technical solutions architecture and support the design, deployment, configuration and monitoring/evaluation of infrastructure, networking, applications, data platform and solution administration; conducts analysis and provides expert support to the planning and conduct of migration projects;
k) Ensure that project Solution Architects follow all aspects of the Enterprise Technical Solution Architecture Process from initiation to closure;
l) Provide architectural consulting expertise, direction, and assistance to systems analysts, IT Cloud engineers, and other systems architects;
m) Manage the portfolio of projects engaged with enterprise information architecture; and
n) Responsible for guidance on High Level Solutions approach and overall Enterprise Information Solution Architecture patterns.

Minimum Qualifications:

a) Post-secondary diploma/degree in Computer Science, Computer Engineering, Information Technology or equivalent;
b) Proven experience as a Solution Architect or in a similar role;
c) Agile/Scrum experience as a Developer or an Architect;
d) Knowledge of coding languages and databases;
e) Strong problem-solving skills and strategic thinking;
f) Cloud architecture experience; and
g) Excellent communication skills with ability to explain technical and security concepts to non-technical audiences.

Role #36 - Business Analyst

Responsibilities:

a) Requirements elicitation and documentation in various formats (i.e., User stories, Business Requirements Document (BRD) etc) for considered alternatives;
b) Perform business analyses of functional requirements to identify information, procedures, and decision flows;
c) Evaluate existing procedures and methods, identify and document items such as database content, structure, integrated application subsystems;
d) Analyze and map the existing business model and the operations, identify areas with scope for improvement.
e) Analyze and evaluate existing business process
f) Define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems;
g) Establish acceptance test criteria with client;
h) Develop and establish service level agreements;
i) Assist in the formalization of business process standards;
j) Support and use the selected organizational methodologies;
k) Assist in the development of organizational methodologies and tools;
l) Analyze and develop of business success "critical success factors";
m) Analyze and develop of architecture requirements design, process development, process mapping and training;
n) Responsible for leading other functional staff to define business strategy and processes in support of transformation and change management activities;
o) Participate in change impact analysis and change management activities;
p) Participate in organizational realignment;
q) Coordinate development of training and coordination with other stakeholders; and
r) Create presentations and present to various stakeholders and facilitate meetings and discussions.

Minimum Qualifications:

a) Previous relevant experience as a Business Analyst;
b) Experience working in Azure Devops or similar environments;
c) Ability to use Microsoft SQL Server Management Studio to review data; and
d) Understanding SQL scripts and PowerShell scripts.

Role #37 – Application Developer

Responsibilities:

a) Understand client requirements and how they translate in application features;
b) Collaborate with a team of IT professionals to set specifications for new applications;
c) Design creative prototypes according to specifications;
d) Write high quality source code to program complete applications within deadlines;
e) Perform unit and integration testing before launch;
f) Conduct functional and non-functional testing;
g) Troubleshoot and debug applications;
h) Evaluate existing applications to reprogram, update and add new features; and
i) Develop technical documents and handbooks to accurately represent application design and code .

Minimum Qualifications:

a) Post-secondary diploma/degree in a related field; and
b) Previous relevant experience as an Application Developer.

Role #38 - Azure Cloud Application Developer

Responsibilities:

a) Support the design, build, configuration, testing, deployment, management and optimization of secure web applications, connectors and services in relation to both on prem and Cloud applications in MS Azure;
b) Assist with updates, functionality testing, scripts and reporting;
c) Troubleshoot problems, determe root cause and deploy solutions;
d) Assist other developers, analysts, and designers in conceptualizing and developing programs and applications;
e) Run and monitor software performance tests on new and existing programs for the purposes of correcting errors, isolating areas for improvement, and general debugging;
f) Ensure backup and disaster recovery for all Azure resources;
g) Research and document requirements of software users;
h) Support the design, build, configuration, testing, deployment, management and optimization of secure web applications, connectors and services in relation to both on prem and Cloud applications in MS Azure;
i) Manage and/or provide guidance to junior developers and research assistants;
j) Recommend, schedule, and perform software improvements and upgrades; and
k) Architect applications for ease of maintenance and longevity.

Minimum Qualifications:

a) Post-secondary diploma/degree in Computer Science, Computer Engineering, Information Technology or equivalent;
b) Microsoft Azure Certifications**;**
c) Previous relevant experience in the role;
d) Experience developing with Cloud APIs;
e) Experience deploying and supporting an infrastructure in a Cloud based on Amazon Web Services (AWS), Azure, etc.;
f) Multi-threading applications;
g) Asynchronous processing of events;
h) NoSQL databases like MongoDB;
i) Web Services;
j) Experience refactoring legacy systems for Cloud;
k) Agile/ Scrum experience ;

l) Microsoft Certified Azure Developer Associate or equivalent Microsoft web certification; and
m) Experience in ASP.Net Core and Visual Studio.

Role #39 – Quality Assurance (QA) Tester
Responsibilities:
a) Create test plans and coordination; b) Supervise testing in accordance with the plan; c) Develop and execute test cases under varying circumstances; d) Document, evaluate test results and reports on the status; e) Establish and maintain source and object code libraries for a multi-platform, multi-operating system environment; f) Establish software testing procedures for unit test, integration testing and regression testing with emphasis on automating the testing procedures; g) Establish and operate "interoperability" testing procedures to ensure that the interaction and co-existence of various software elements, which are proposed to be distributed on the common infrastructure, conform to appropriate organizational standards (e.g. for performance, compatibility, etc.) and have no unforeseen detrimental effects on the shared infrastructure; h) Establish a validation and verification capability which assumes functional and performance compliance; i) Manage and monitor test plans for all levels of testing; j) Manage of walkthroughs and reviews related to testing and implementation readiness; k) Develop and maintenance of QA standards and methodologies; and l) Develop of QA/testing manuals, procedures, and performance measurement tools.
Minimum Qualifications:
a) Post-secondary diploma/degree in a related field; and b) Previous relevant experience as a QA tester.

9. The following are the specific descriptions for each Role in Service Category #9 - Business Intelligence and Analytics:

Role #40 - Business Intelligence Developer
Responsibilities:
a) Design, develop, implement, and maintain BI solutions such as reports, dashboards, and data warehouses; b) Design and implement ETL/ELT processes, and data integration from a variety of sources to ensure that the data warehouse is populated with clean, consistent, and reliable data; c) Collaborate with business users and stakeholders to understand their requirements and translate them into data-driven solutions; d) Use data visualization tools and software to provide clear reporting and actionable insights; e) Develop and maintain documentation related to the organization's data architecture, data dictionary, or database design and structure; f) Ensure data quality and integrity by implementing effective data management processes; g) Develop and manage BI processes to improve data collection and reporting efficiency; h) Collaborate with data engineers and IT team to ensure data sources are reliable and accessible; i) Provide training and support to business users on BI tools and systems; j) Stay up to date with the latest industry trends and technologies to continually improve BI solutions; k) Evaluate the effectiveness of the current BI tools and processes and recommend improvements or new technologies as needed; l) Establish governance and control policies to ensure that business intelligence activities comply with regulatory standards and best practices; m) Collaborate closely with other teams, such as Data Science, IT, and Operations, to ensure that the BI solutions meet the needs of the organization as a whole; n) Perform regular system audits and performance monitoring to ensure the optimal functioning of the BI systems and tools; o) Act as a mentor to junior BI Developers or other team members, sharing knowledge and expertise.

p) Manage the lifecycle of the BI solutions, including the sunset of outdated reports and the transition to new systems; and
q) Proactively identify potential data issues and work with cross-functional teams to correct and prevent them in the future.

Minimum Qualifications:

a) Post-secondary diploma/degree in Computer Science, Information Systems, or a related field;
b) Previous relevant experience as a BI/DW Specialist;
c) Strong knowledge of BI technologies (e.g., Microsoft Power BI, Tableau);
d) Database experience (SQL Server);
e) Experience with database design and data warehousing;
f) Strong analytical skills with a focus on ensuring data accuracy and integrity;
g) Ability to translate business needs into technical specifications;
h) Excellent problem-solving skills and attention to detail; and
i) Strong communication and interpersonal skills.

Role #41 - Data Architect

Responsibilities:

a) Responsible for the overall data architecture, continuous development, operation, and maintenance of data services and analytic tools;
b) Acquire stakeholder requirements and envision optimal data solutions that encourage long-term compatibility, scalability and maintainability;
c) Design and implement data products including data models, dashboards and visualizations required to meet the organization's objectives;
d) Develop and apply standardization methods to integrate data from numerous sources into corporate data systems, ensuring data integrity and interoperability with existing corporate applications and business intelligence solutions;
e) Manage the BI dependency plan, job scheduling and product release-cycle;
f) Monitor performance and business use of data systems to identify areas of opportunities for optimization and enhancements;
g) Monitor industry trends, identifying and evaluating emerging data technologies, services, standards and strategies;
h) Promote the benefit of standardized business intelligence tools and methodologies across the organization;
i) Implement effective metadata management processes and oversee the mapping of data sources, data movement, and data quality;
j) Develop and implement data governance and data security strategies, adhering to compliance requirements;
k) Work closely with IT team, data scientists, analysts, and business stakeholders to ensure the data architecture aligns with and supports business requirements;
l) Assess the impact of new business requirements on the existing data architecture and suggest suitable solutions; and
m) Use Microsoft Azure services for data storage, data integration, data processing, and analytics as required.

Minimum Qualifications:

a) An undergraduate degree in Computer Science, Information Systems, or a related field;
b) Proven work experience as a Data Architect, Data Scientist, Data Analyst or similar role;
c) Experience with Microsoft Azure Data and Analytics Stacks;
d) Strong knowledge of database structure systems and data mining;
e) Excellent understanding of data administration and management functions;
f) Familiarity with modern data technologies and ETL tools;
g) Knowledge of data visualization and analytics tools;
h) Proficiency in SQL and other data languages;
i) Strong problem-solving and analytical skills; and
j) Excellent communication and collaboration skills.

Role #42 - Data Scientist
Responsibilities:
a) Work closely with statisticians to identify, design, and build appropriate datasets for complex experiments; b) Establish links across existing data sources and find new, interesting mash-ups; c) Develop algorithms and predictive models to solve critical business problems; d) Develop tools and libraries that will help analytics team members more efficiently interface with huge amounts of data; e) Create informative visualizations that intuitively display large amounts of data and/or complex relationships; f) Drive the collection of new data and the refinement of existing data sources; g) Analyze large, noisy datasets and identify meaningful patterns that provide actionable results; h) Create data mining and analytics architectures, coding standards, statistical reporting, and data analysis methodologies; i) Coordinate data resource requirements between analytics team and engineering teams; j) Assist in the development of data management policies and procedures; k) Develop best practices for analytics instrumentation and experimentation; l) Conduct research and make recommendations on big data infrastructure, database technologies, analytics tools, services, protocols, and standards in support of procurement and development efforts; m) Develop and automate new enhanced imputation algorithms; n) Provide and apply quality assurance best practices for data science services across the organization; o) Develop, implement, and maintain change control and testing processes for modifications to algorithms and data analytics; p) Manage and/or provide guidance to junior members of the analytics team; q) Collaborate with team members and stakeholders to implement models and monitor outcomes; and r) Maintain updated knowledge of data analysis, machine learning, and industry best practices.
Minimum Qualifications:
a) Post-secondary diploma/degree in the field of Computer Science, Information Systems, or Computer Engineering and/or twelve (12) years equivalent work experience; b) Working technical experience with developing, installing, configuring and supporting multi-terabyte database environments; c) Strong understanding of relational database structures, theories, principles, and practices; d) Hands-on experience with business requirements gathering/analysis; e) Previous relevant data scientist or quantitative modeling experience; f) Experience with database and dataset (SQL, NoSQL, etc.) and data visualization tools (e.g., Tableau, PowerBI, etc.); g) Strong problem-solving skills with an emphasis on product development; and h) Excellent communication and presentation skills with the ability to translate complex results into a compelling narrative.

10. The following are the specific descriptions for each Role in Service Category #10 – ServiceNow Development:

Role #43 - ServiceNow Developer
Responsibilities:
a) Actively participate in agile daily scrums, documenting development progress and collaborating across platform teams; b) Ensure that all development adheres to ServiceNow development standards; c) Support in the development of use cases and testing procedures, ensuring product functionality, debugging and testing is completed prior to production deployment; d) Build automated testing in ServiceNow Automated Test Framework (ATF);

e) Maintain existing ATF framework and ensure that ATF scripts are kept current;
f) Validate/Test API integrations;
g) Collect and report quality metrics from test execution;
h) Analyze software and systems before customer use to ensure the product is defect-free.
i) Validate functionality build by Developers and/or 3rd party vendors;
j) Support and participate in customer requirement workshops, working with product owner/stakeholders to configure/develop requested items and tasks;
k) Work with project teams to understand business/system requirements and solution designs and handle multiple priorities simultaneously;
l) Design, create and configure Notifications, User Interface (UI) Pages, UI Macros, Script Includes, Formatters, etc.;
m) Design, create and configure Business Rules, UI Policies, UI Actions, Client Scripts including advanced scripting of each;
n) Create and maintain system design and operations documentation; and
o) Deliver reporting solutions using Performance Analytics (PA) or standard dashboard reporting.

Minimum Qualifications:

a) An undergraduate degree in Computer Science or relevant, proven industry experience;
b) Minimum of three (3) years' experience integrating ServiceNow with external systems;
c) Minimum of three (3) years' experience with HTML5, JavaScript, jQuery;
d) Extensive understanding of the ways in which ServiceNow can be configured and customized and scripting within the tool;
e) Knowledge of building ATF scripts and maintaining the framework as changes take place within the modules, apps and forms; and
f) Experience with development in ServiceNow platform.

Role #44 – ServiceNow Implementation Specialist

Responsibilities:

a) Design and configure ServiceNow Product suites as part of a cross-functional team;
b) Develop User Interface (UI) forms, fields, notifications and workflows;
c) Create, monitor, modify both simple and advanced workflows aligned to best practices for the betterment of processes and strategies (considering scalability, performance, business policies and future needs);
d) Create new catalog requests and items with multiple variables;
e) Create and maintain access control list (ACL), groups and roles;
f) Develop and maintain custom scripts;
g) Configure and maintain data imports sets and software integrations;
h) Complete unit and regression testing;
i) Coordinate with development team to develop custom applications and/or integration to a variety applications;
j) Coordinate with system administrators to apply ServiceNow patches/releases to instances; and
k) Assist in troubleshooting instance and continuously improve configuration to improve employee experience and efficiency.

Minimum Qualifications:

a) ServiceNow configuration experience (preferred) or relevant and transferable enterprise level experience with SaaS;
b) Experience in either a business analysis or technical capacity at an enterprise level (range of experience years; 3-5 years);
c) Three (3) years' experience with agile methodology and software; and
d) Working knowledge of relational databases.

Role # 45 – ServiceNow Solution Architect
Responsibilities:
a) Identify opportunities for improvement within existing service operations and core propositions related to ServiceNow; b) Proactively bring thought leadership and business outlook to effectively address client issues/demands related to ServiceNow solutions; c) Manage the delivery of ServiceNow projects, coordinating with teams and providing technical expertise and guidance; d) Work closely with other technical architects and business leads at a detailed project level, to ensure that the agreed design principles and standards are embedded into the ServiceNow solutions throughout the service delivery lifecycle; e) Consult on, design, and lead development of integrations between ServiceNow and other enterprise tools; f) Contribute to the definition of ServiceNow design policies, principles and guidance and the continuous improvement of working practices; g) Lead and participate in development squads following common methodologies including Agile; h) Contribute to the development and enhancement of working cost models for ServiceNow related solutions; and i) Mentor and train colleagues of ServiceNow capabilities, solutions and offering.
Minimum Qualifications:
a) Understand ITIL and architecture frameworks/methods; b) Certified ServiceNow System Administrator and Implementation Specialist; c) Understanding of Agile delivery methodologies; d) Minimum of five years' experience within the IT services industry, at least two which have involved ServiceNow solutions; e) Experience of developing ServiceNow managed service solutions and propositions; and f) Experience developing ServiceNow solution strategies, governance models and SLA framework.

[END OF APPENDIX "A-1" (SERVICE STREAM #1: STAFF AUGMENTATION SERVICES, SERVICE CATEGORIES AND ROLES)]

Appendix "A-2"

Service Stream # 2: Project Delivery Services, Service Categories Description

Projects undertaken by CDIC under Service Stream # 2 may require either an individual resource or a team of resources to work with CDIC.

The following is a list of the eight (8) Service Categories applicable to this Service Stream.

#	Service Category
1	Strategy
2	Architecture
3	Security and Risk
4	Infrastructure
5	Business Application Solutions
6	Salesforce Development
7	Business Intelligence and Analytics
8	ServiceNow Solutions

The following is the description for Service Category #1 - Strategy:

Service Category #1 - Strategy
Description:
Strategy projects will contribute to the development of strategies intended to improve services and operations for CDIC. The requested project(s) may include but are not limited to: IT Strategy; Data Strategy; Cloud Strategy; Security Strategy; and Modernization Strategy.

The following is the description for Service Category #2 – Architecture:

Service Category #2 - Architecture
Description:
Architecture projects will translate organizational goals and objectives into architecture requirements, solutions and changes. The requested project(s) may include but are not limited to: Technology Roadmaps; Solution Architectures; and Enterprise Architectures.

The following is the description for Service Category #3 – Security and Risk:

Service Category #3 - Security and Risk
Description:
Security and Risk Projects will assess and manage risks for CDIC's information systems. The requested project(s) may include but are not limited to: Security Assessments and Reviews; Security Management; Risk Audits; Security Audits; Penetration Testing, and Vulnerability Scanning.

The following is the description for Service Category #4 – Infrastructure:

Service Category #4 - Infrastructure
Description:
Infrastructure projects will rationalize, standardize and structure CDIC's IS Infrastructure landscape. This incorporates the on and/or off-premise technology that supports CDIC. The requested project(s) may include but are not limited to: Cloud Migration; Asset Management; Infrastructure Modernization/Upgrades; and Business Continuity Planning/Disaster Recovery Planning (BCP/DRP).

The following is the description for Service Category #5 – Business Application Solutions:

Service Category #5 - Business Application Solutions
Description:
Business Application solution projects will identify business problems or opportunities and transform into a new application, upgrade existing applications or provide support for existing applications. The requested project(s) may include, but are not limited to; strategizing, designing, developing and managing CDIC's applications based on business user requirements.

The following is the description for Service Category #6 – Salesforce Development:

Service Category #6 - Salesforce Development
Description:
Salesforce Development projects may include, but are not limited to; assessing business objectives and needs and translate them into solutions in the Salesforce platform. The requested project(s) may, but are not limited to: focus on improving the workflow and user experience, configurations, customization and development of applications.

The following is the description for Service Category #7 – Business Intelligence and Analytics:

Service Category #7 - Business Intelligence and Analytics
Description:
Business Intelligence and Analytics initiatives related to the creation of new data products including, but not limited to, dashboards, reports, repositories, machine learning applications, upgrade of existing applications and provision of support for existing applications. The requested project(s) may include, but are not limited to, strategizing, designing, developing and managing CDIC's applications based on business user requirements.

The following is the description for Service Category #8 – ServiceNow Solutions:

Service Category #8 – ServiceNow Solutions
Description:
ServiceNow projects may include, but are not limited to, assessing business objectives and translating them into solutions in the ServiceNow platform. The requested project(s) may include, but are not limited to: gathering requirements, identifying use cases, defining architecture including integration, configuring, testing and deploying the solution(s).

[END OF <u>APPENDIX "A-2"</u> (SERVICE STREAM #2: PROJECT DELIVERY SERVICES, SERVICE CATEGORIES)]

Schedule "B"

Evaluation and Selection Process

Selection Method

Proposals must comply with the requirements of the RFSA to be deemed responsive. Without limiting Section 11, CDIC's Reserved Rights of the RFSA, CDIC may, in its sole and absolute discretion, reject or refuse to consider any Proposal if CDIC determines that the information, statements or supporting material in the Technical Offer or in the Financial Offer are inconsistent with, or otherwise fails to respond to, any of the requirements of the RFSA.

CDIC is seeking to establish up to twenty (20) Supply Arrangements for Service Stream #1: Staff Augmentation Services and there is an unlimited number of Supply Arrangements for Service Stream #2: Project Delivery Services.

CDIC expects Bidders will only submit one Proposal in response to the RFSA. Bidders can do so either as a partnership (i.e., Company AB in partnership) or single entity/Bidder (i.e., Company A), but not both. The same Bidder will not be permitted to submit, or be part of, more than one Proposal.

All Proposals will be examined in accordance with the following process:

Step 1: Confirmation of Compliance with the Mandatory Requirements

Technical Offers will be reviewed for substantial completeness and compliance with the **Mandatory Requirements** described in Schedule "E" (Required Forms) of the RFSA, to confirm that the information, statements and supporting material in the bidder's Technical Offer substantiate a compliant response. Subject to CDIC's reserved rights (including those in Section 11, CDIC's Reserved Rights), any Proposal that is not considered by CDIC to be in substantial compliance with all Proposal requirements and all other Mandatory Requirements, as confirmed on a pass or fail basis, may be disqualified and not given further consideration in this process.

Step 2: Evaluation of Rated Requirements – Business Experience and Expertise (100 points)

Technical Offers will be evaluated against the Rated Requirements outlined in Part 1 of Appendix "C-1" (Technical Offer) of the RFSA and will consist of an evaluation of the business experience and expertise of the Bidder. Technical Offers will be assigned a score for each Rated Requirement to establish a Step 2 "**Technical Score**". The maximum Technical Score for Step 2 is one hundred (100**)** points. Bidders must achieve a minimum Technical Score of seventy (70) points to proceed to Step 3 and be given further consideration in this process.

At the end of this Step 2 (Evaluation of Rated Requirements – Business Experience and Expertise), CDIC will establish a shortlist of bidders that achieve a Step 2 Technical Score of at least seventy (70) points out of the one hundred (100) total points available. Only the bidders meeting this criterion will be eligible to proceed to the next step of the evaluation and selection process.

The following example of this Step 2 is for illustration purposes only; any differences between this example and the values as set out in this RFSA are intentional:

Bidder	Step 2 Technical Score (Maximum of 100 points)
Bidder A	90
Bidder B	55
Bidder C	91
Bidder D	85
Bidder E	83
Bidder F	69

As a result, only Bidders A, C, D, and E will be shortlisted and proceed to the next step. Bidders B and F are not eligible to be given further consideration as they did not achieve the minimum Step 2 Technical Score of seventy (70) points.

Step 3: Evaluation of Rated Requirements — Technical Experience and Expertise - Reference Engagements (200 Points per Service Category)

Each Service Category will be evaluated separately and independently from one another.

Technical Offers shortlisted from Step 2 will be evaluated against the Rated Requirements outlined in Part 2 of Appendix "C-2" (Reference Engagement Form) of the RFSA, and will consist of an evaluation of the bidder's technical experience and expertise for the Service Category being proposed in the bidder's Technical Offer.

All bidders are required to submit two (2) Reference Engagement Forms for each Service Category for which they are offering their services.

The bidder must demonstrate its ability to provide services in one or more Service Categories under one or both of the two (2) Service Streams in Schedule "A" (Statement of Work). The bidder must provide two (2) completed Reference Engagement Forms for each Service Category being offered under a Service Stream in order for the bidder's offer for that Service Category to be qualified. If the bidder does not include two (2) completed Reference Engagement Forms for each Service Category, including for any Service Category with only one Role, its offer for that Service Category will be disqualified.

At the end of this Step 3 (Evaluation of Rated Requirements – Technical Experience and Expertise -Reference Engagements), CDIC will establish a shortlist of bidders that have achieved a minimum Technical Score of at least seventy (70) points out of the one hundred (100) points available for each of the two (2) Reference Engagement Forms for each applicable Service Category. Any Reference Engagement Form that does not achieve seventy (70) points will receive a "fail" and Bidder's Proposal for that Service Category will not be given further consideration in this process.

Bidders must qualify for at least one Service Category under a Service Stream to be qualified for the Service Stream.

The following example of this Step 3 is for illustration purposes only; any differences between this example and the values as set out in this RFSA are intentional:

Bidder	**Step 3 Technical Score (Maximum of 200 points) Service Category #1**		**Step 3 Technical Score (Maximum of 200 points) Service Category #2**	
	Reference Engagement Form 1	**Reference Engagement Form 2**	**Reference Engagement Form 1**	**Reference Engagement Form 2**
Bidder A	90	85	78	**65 FAIL**
Bidder C	No Bid	No Bid	71	73
Bidder D	85	80	72	85
Bidder E	83	**69 FAIL**	No Bid	No Bid

For Service Category #1, as a result of the evaluation process, only Bidders A and D will proceed to the next step. Bidder E did not achieve the minimum Step 3 Technical Score of seventy (70) points and is therefore not eligible to be given further consideration, while Bidder C did not submit a Technical Offer for Service Category #1.

For Service Category #2, as a result of the evaluation process, only Bidders C and D will proceed to the next step. Bidder A did not achieve the minimum Step 3 Technical Score of seventy (70) points and is therefore not eligible to be given further consideration, while Bidder E did not submit a Technical Offer for Service Category #2.

For clarity, as each Service Category is evaluated separately and independently from one another, it is possible for a Bidder to proceed to the next step in the evaluation process for one Service Category and not for the other.

INSTRUCTIONS FOR BIDDERS FOR STEP 3:

The bidder must provide two (2) completed Reference Engagement Forms for the Service Category being offered (one Reference Engagement Form for each of two (2) independent and distinct Engagements), according to the instructions contained in the form.

The bidder must provide details in each of the two (2) Reference Engagement Forms of its experience and expertise as it relates to the particular Service Category for which the bidder is submitting a Technical Offer. Scoring of the Reference Engagement Form will be based on how well the Proposal demonstrates the bidder's technical experience and expertise in relation to the requirements in the RFSA and the level of detail of the Reference Engagement Forms provided. Information provided elsewhere in the Proposal may not be considered in the evaluation of Step 3 of this RFSA.

If a bidder submits fewer than two (2) Reference Engagement Forms for a particular Service Category, bidder's Proposal will not be given further consideration for that particular Service Category.

Therefore, a bidder submitting a Proposal for Service Stream #1 for both Service Category #1 and Service Category #2 must, in order to meet Step 3 Requirements, submit a total of four (4) Reference Engagement Forms (two (2) Reference Engagement Forms for each Service Category).

Step 4: Evaluation of Financial Offers

Financial Offers will be reviewed for substantial completeness and compliance with the **Financial Offer Requirements** described in Schedule "D" (Financial Offer Requirements and Evaluation) of the RFSA, to confirm that the information, statements and supporting material in the Bidder's Financial Offer substantiate a compliant response, subject to CDIC's reserved rights (including those in Section 11, CDIC's Reserved Rights)

Step 5: Ranking and Selection of Successful Bidders

At the end of Step 4, it is CDIC's intent to recommend for award up to twenty (20) Supply Arrangements with bidders having met the minimum points in Step 3 to provide Services in a Service Category for Service Stream #1: IT Staff Augmentation, without limitation to any other provision of this RFSA, including but not limited to Section 11 CDIC's Reserved Rights. There is no limit to the number of recommendations for award for Service Stream #2: Project Delivery Services.

For clarity, as each Service Category is evaluated separately and independently from one another, it is possible for a Bidder to proceed to the next step in the evaluation process for one Service Category and not for the other.

Step 6: Negotiations

If the recommendation is approved, CDIC will enter into negotiations with the successful Bidder(s) to finalize an agreement in accordance with this RFSA, prior to proceeding with the award(s).

Failure to Enter into Agreement

Bidders acknowledge and agree that CDIC does not represent or warrant that they will be able to conclude an agreement and has no obligation to conclude an agreement. If the parties cannot conclude negotiations and finalize the agreement for the Services, CDIC may determine at any time, in its sole and absolute discretion to

discontinue negotiations with any top-ranked bidder and may invite the next-best-ranked bidder to enter into negotiations. This process will continue until an agreement is finalized, until there are no more bidders remaining that are eligible for negotiations or until CDIC elects to cancel the RFSA process.

Evaluation Point Allocation Chart

The following tables show a summary of the evaluation steps and methodology for this RFSA:

Steps	Description	Maximum Points	Minimum Points Required
1	**Substantial Completeness and Mandatory Requirements**	Pass	**Pass**
2	**Technical Offer** **Part 1 of Appendix "C-1"** **(Technical Offer)** Business Experience and Expertise (Rated)	**100** points	**70** points (70%)
3	**Reference Engagement Forms** **Part 2 of Appendix "C-1"** **(Technical Offer)** Technical Experience and Expertise (Rated) **(Appendix "C-2" (Reference Engagement Form))**	**200** points 100 points for each Reference Engagement Form	Consisting of a minimum of 70 points (70%) for each Reference Engagement Form

Scoring Methodology

The following is the basis for the scoring method that will be applied to the Rated Requirements in Appendix "C-1" (Technical Offer) and Appendix "C-2" (Reference Engagement Form):

Score	Rationale
5	Fully meets and/or exceeds CDIC's requirement. No weaknesses exist. A comprehensive response with no significant gaps.
4	Very Good, substantially meets CDIC's requirement. Strengths exceed weaknesses, and weaknesses are easily correctable.
3	Acceptable, meets the basic requirement of CDIC. There may be strengths or weaknesses, or both. Weaknesses do not significantly impact the requirements and are correctable.
2	Marginal, falls short of meeting the basic requirement of CDIC. Weaknesses exceed strengths and will be difficult to correct.
1	Unacceptable, minimal response, e.g., statement of compliance with no substantiation. Noted deficiencies are expected to be very difficult to correct or are not correctable.
0	Unresponsive, no relevant response / unsatisfactory.

[END OF SCHEDULE "B" (EVALUATION AND SELECTION PROCESS)]

Schedule "C"

Technical Offer Submission Form

INSTRUCTIONS TO BIDDERS: Technical Offer Submission Form should be accompanied by Appendix "C-1" (Technical Offer) and all applicable Appendix "C-2" (Reference Engagement Form(s)), for each Service Category being offered under the Service Stream(s).

TECHNICAL OFFER

LEGAL NAME OF BIDDER: _____

ADDRESS: _____

CONTACT NAME: _____

TELEPHONE: _____

EMAIL: _____

SOLICITATION NUMBER: **RFSA 2023-3941**

TITLE: **Information Technology Staff Augmentation and Project Delivery Services**

1. The undersigned, as the authorized representative of the bidder (hereinafter referred to as the **Bidder")** hereby offers to the Canada Deposit Insurance Corporation ("**CDIC**") all necessary goods, services, labour, superintendence, supplies and facilities, and pursuant to the above solicitation, warrants and certifies:

   i. It has not, directly or indirectly, paid or agreed to pay, and will not, directly or indirectly, pay, a contingency fee to any individual for the solicitation, negotiation or obtaining of the Agreement if the payment of the fee would require the individual to file a return under section 5 of the *Lobbying Act*; and
   ii. It has not been convicted of an offence under section 121, 124 or 418 of the *Criminal Code* other than an offence for which a pardon has been granted.

2. Ability to Provide Deliverables

   The Bidder has carefully examined the RFSA documents and has a clear and comprehensive knowledge of the Services required. The Bidder represents and warrants its ability to provide the Services in accordance with the requirements of the RFSA for the rates set out in its proposal.

3. Acknowledgment of Non-Binding Procurement Process

   The Bidder acknowledges that the RFSA process will be governed by the terms and conditions of the RFSA, and that, among other things, such terms and conditions confirm that this procurement process does not constitute a formal, legally binding bidding process (and for greater certainty, does not give rise to a contract, a bidding process contract), and that no legal relationship or obligation regarding the procurement of any good or service will be created between CDIC and the Bidder unless and until CDIC and the Bidder execute a written agreement for the Services.

4. No Prohibited Conduct

   the Bidder declares that it has not engaged in any conduct prohibited by this RFSA.

5. Conflict of Interest

The Bidder must declare all potential Conflicts of Interest. This includes disclosing the names and all pertinent details of all individuals (employees, advisers, or individuals acting in any other capacity) who (a) participated in the preparation of the proposal; **AND** (b) were employees of CDIC within twelve (12) months prior to the Deadline for Proposals.

If the box below is left blank, the Bidder will be deemed to declare that (a) there was no Conflict of Interest in preparing its proposal; and (b) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the RFSA.

Otherwise, if the statement below applies, check the box.

☐ The Bidder declares that there is an actual or potential Conflict of Interest relating to the preparation of its proposal, and/or the bidder foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the RFSA.
If the Bidder declares an actual or potential Conflict of Interest by marking the box above, the Bidder must set out below details of the actual or potential Conflict of Interest:

_____
_____
_____
_____

6. Disclosure of Information

The Bidder hereby agrees that any information provided in this proposal, even if it is identified as being supplied in confidence, may be disclosed where required by law or by order of a court or tribunal. The Bidder hereby consents to the disclosure, on a confidential basis, of this proposal by CDIC to the advisers retained by CDIC to advise or assist with the RFSA process, including with respect to the evaluation this proposal.

By signing this Form the Bidder represents that the above information is true as of the date indicated below and will continue to be true for the duration of any resulting Contract. Bidder understands that the certifications provided to CDIC are subject to verification at all times, and further understands that CDIC will declare a contractor in default, if a certification is found to be untrue, whether made knowingly or unknowingly, during the solicitation or contract period. CDIC reserves the right to ask for additional information to verify the certifications. Failure to comply with any request or requirement imposed by CDIC will constitute a default under any resulting Contract.

_____ _____

Bidder Signature Date

_____ _____

Print Name Title

I have authority to bind the Bidder.

PROPOSALS WHICH DO NOT CONTAIN THE REQUESTED DOCUMENTATION MAY BE DEEMED NON-COMPLIANT.

[END OF SCHEDULE "C" (TECHNICAL OFFER SUBMISSION FORM)]

Appendix "C-1"
Technical Offer

INSTRUCTIONS TO BIDDERS: The bidder must not alter the format of the table below in any way, other than to remove highlighted text and add hard returns to provide responses. Columns and rows are not to be added or deleted.

Part 1 – Business Experience and Expertise - Rated Requirements (Maximum Points – 100 Points)

Applicable to all Service Streams (one Technical Offer per bidder).

Section 1. Bidder Information – Not Rated **Bidder should provide the following information**	
a) Bidder's Legal Name:	[Insert legal name]
b) Number of years the bidder has been in business:	[Insert years in business]
c) Number of employees employed by the bidder (identify the number of full-time, part-time and contract personnel):	
(Maximum of 200 words)	
d) Description of the corporate history of bidder, including any acquisitions or divestitures over the last ten (10) years:	
(Maximum of 500 words)	
e) Location of each of the bidder's offices, including number of staff at each location and their primary functions:	
(Maximum of 500 words)	

Section 2. Bidder's Technical Offer **The bidder should identify the Service Stream(s) for which bidder is submitting a Proposal by placing an "X" in one or both of the applicable boxes.**
☐ **1. Service Stream #1: Staff Augmentation**
☐ **2. Service Stream #2: Project Delivery Service**

Section 3. Rated Requirements

Part 1 – Rated Requirements (Maximum Points – 100)

Applicable to all Streams (one Technical Offer per bidder).

RR1. Organizational Experience – (Maximum Points – 30)

Bidder should clearly describe the organization's knowledge, qualifications and expertise in relation to the proposed Service Stream(s) the bidder is offering as part of its Proposal.

In its response, bidder should clearly demonstrate, at a minimum:

a) *A clear description of how such knowledge, qualifications and expertise are aligned with CDIC's requirements for each Service Stream(s) the bidder will be offering as part of its Proposal; and*

b) *Experience in the public sector related to each Service Stream(s) the bidder will be offering as part of its Proposal.*

A1. *(Maximum of 1,000 words)*

RR2. Understanding and Approach – (Maximum Points – 10)

Bidder should describe its understanding of CDIC's requirements in relation to the Service Stream(s) the bidder is offering as part of its Proposal, and the bidder's approach to meeting CDIC's requirements.

In its response, bidder should clearly demonstrate:

a) *How the bidder plans to establish and maintain an effective working relationship with CDIC;*

b) *How the bidder will collaborate with CDIC and manage feedback and changes;*

c) *How the Bidder will handle any issues that may arise between the bidder and CDIC; and*

d) *Any escalation and complaint resolution mechanism and/or procedures applicable to each proposed Service Stream.*

A2. *(Maximum of 500 words)*

RR3. Key Personnel Qualifications – (Maximum Points – 10)

In relation to the services described under the Service Stream(s) the bidder is offering as part of its Proposal, the bidder should:

a) *Clearly identify the proposed key client relationship lead(s), including who will serve as the key point of contact for each applicable Service Stream, and clearly describe any other roles and resources that would be involved in providing such services to CDIC;*

b) *For the key client relationship lead(s) that the bidder proposes to assign to CDIC for the delivery of the services identified for each respective Service Stream, and for any proposed alternate, provide a resumé*

that includes the number of years of experience providing services such as those required for the engagement with CDIC, including specific examples of experience; and

c) *Clearly identify and describe the bidder's approach to maintaining its relationship with CDIC in the event that a change of key client relationship lead(s) and/or key point of contact occurs, on either an interim or an ongoing basis.*

A3. *(Maximum of 500 words, excluding resumé(s))*

RR4. Ongoing Access to Resources – (Maximum Points – 10)

Bidder should clearly describe for each of the Service Stream(s) the bidder is offering as part of its Proposal:

a) *How the bidder will retain ongoing access to qualified resources to meet immediate and future CDIC requirements; and*

b) *How the bidder will cover for any absences and/or departures of resources during the performance of the services. The bidder should clearly describe its current resource management framework and explain how it will be applied.*

A4. *(Maximum of 500 words)*

RR5. Quality Assurance and Service Levels – (Maximum Points – 10)

Bidder should clearly describe its approach to quality assurance and service levels, and address the following as part of its response:

a) *Approach to quality assurance for the performance of the services for each proposed Service Stream;*

b) *How the quality assurance approach will be consistent throughout the duration of the Supply Arrangement for each proposed Service Stream, including such approach for any subcontractors (if applicable); and*

c) *Any service levels for each proposed Service Stream that meets or exceeds CDIC's requirements, including any processes it has in place to measure performance of bidder and any subcontractor(s) against such service levels.*

A5. *(Maximum of 500 words)*

RR6. Environmental, Social and Governance – (Maximum Points – 10)

Bidder should clearly describe its approach to including Environmental, Social and Governance considerations in its operations and in the delivery of services, by describing, at a minimum, the following elements in its response:

a) *Hiring practices in support of diversity, inclusion and equity;*

b) *Measures taken to identify and remove barriers and increase accessibility for persons with disabilities; and*

c) *Practices and/or measures taken in support of the environment, including reducing its organization's carbon footprint and green procurement.*
A6. *(Maximum of 1,000 words)*
RR7. Information Security – (Maximum Points – 20) *Bidder should clearly describe, at a minimum:* a) *Its methodology and approach to collecting CDIC data and maintaining data security throughout the duration of the Supply Arrangement, including reassurances that any CDIC data collected by bidder, its personnel or any subcontractors will only be stored in Canada.*
A7. *(Maximum of 500 words)*
Part 2 – Service Stream Specific Technical Experience and Expertise - Rated Requirements - Reference Engagements – (Maximum Points – 100 Points per Reference Engagements) **Each Service Category will be evaluated separately. Bidder to complete Appendix "C-2" (Reference Engagement Form).**

[END OF APPENDIX "C-1" (TECHNICAL OFFER)]

Appendix "C-2"

Reference Engagement Form

INSTRUCTIONS TO BIDDERS: Bidders are required to use the form provided in this Appendix "C-2" using only the Service Category name and Role referred in this RFSA for which the Bidder wishes to be qualified.

The Bidder must identify, in Section 1 of the Reference Engagement Form, both the Service Stream and Service Category to which the Reference Engagement Form applies by placing an (X) in the box beside the name of the Service Stream and the applicable Service Category to which the Reference Engagement Form relates, respectively. If the Bidder places an (X) in more than one box, CDIC will only evaluate the Reference Engagement indicated by the first box in which an (X) appears. For a Service Category under Service Stream #1 ONLY, Bidders should also identify at least one (or more) relevant Role(s) by placing an (X) in the box beside the name of the Role(s).

Bidders are NOT required to submit separate Reference Engagements Forms for each of the forty-five (45) Roles under Service Stream #1 or map each Role to their specific responsibilities/ qualifications. Bidders that qualify for a specific Service Category will qualify for ALL Roles for which they have provided a rate in Appendix "D-1" (Financial Offer for Service Stream #1).

Only two (2) Reference Engagement Forms may be submitted for each Service Category. If a Bidder submits more than two (2) Reference Engagement Forms for the same Service Category in its Proposal, CDIC will only evaluate the first two (2) Reference Engagement Forms submitted for that Service Category, in the order in which they appear in the Proposal.

Bidder may not submit the same Reference Engagement more than once in its entire Proposal. For clarity, all Reference Engagement Forms submitted must be for different Engagements. If the Bidder submits the same Reference Engagement more than once, CDIC will only evaluate once, the first time it appears in the Proposal.

All Reference Engagement Forms must reflect Engagements the Bidder has started after January 1, 2020, and prior to the Proposal Submission Deadline. Any Engagement with a start date prior to January 1, 2020, or after the Proposal Submission Deadline will not be given further consideration in this evaluation process. All Reference Engagement Forms may indicate "on-going" as a completion date. For projects that include on-going maintenance and support or other ongoing deliverables; CDIC will only consider the completed portion of the project deliverable. For staff augmentation placements that indicate "on-going", the Engagement should contain a sufficient level of detail with technical experience and expertise in relation to the requirements in the RFSA.

All Reference Engagements must have a dollar value of at least $25,000 CAD OR a statement confirming that the Reference Engagement value was a minimum of $25,000 CAD. Any Reference Engagement that does not have a dollar value of at least $$25,000 CAD OR a statement confirming that the Reference Engagement value was a minimum of $25,000 CAD will not be considered for evaluation and will be disqualified.

All Reference Engagements must have a duration of at least twenty (20) working days. Any Reference Engagement that does not have a duration of at least twenty (20) working days will not be considered for evaluation and will be disqualified.

Engagement Profiles may be for Reference Engagements conducted for clients in either the public or private sector. Private sector related Reference Engagements are not limited to clients within the financial sector/services.

The Reference Engagements are not limited to Engagements completed in Canada. Bidders should provide the applicable information requested that accurately describes their organization as it relates to providing the Services required by CDIC as described in the RFSA.

Without limiting the reserved right of CDIC to verify references other than those provided by the bidder, CDIC, in its sole discretion, may, during this RFSA evaluation process, contact any references to verify the information provided and/or confirm the Bidder's experience and/or ability to undertake the Engagement/provide the services required and described in the bidder's Proposal.

The bidder must not alter the format of the table below in any way, other than to remove highlighted text and add hard returns to provide responses. Columns and rows are not to be added or deleted.

Part 2 – Technical Experience and Expertise - Rated Requirements (Maximum Points – 100 Points per Reference Engagement)

NOTE: Bidder should complete and submit two (2) Reference Engagement Forms for each Service Category.

Bidder's Legal Name:	[Insert legal name of company/firm who provided the services under this Engagement] *"Bidder's Legal Name" provided in the Reference Engagement Form is the same as the Bidder's legal name provided in Schedule "C" (Technical Offer Submission Form) and was responsible for and had control of the work of its personnel and/or subcontractors.*

1. Rated Requirements

The bidder should identify the Service Stream profiled in this Reference Engagement (ONLY 1 Service Stream per Reference Engagement) by placing an "X" in the applicable box.

Service Stream	
☐ **1. Service Stream #1: Staff Augmentation**	☐ **2. Service Stream #2: Project Delivery Services**

The Bidder must identify the Service Category profiled in this Reference Engagement (ONLY 1 Service Category per Reference Engagement) by placing an "X" in the applicable box.

	#	Service Category (SC) #1		#	Service Category (SC) #2
☐	1	Advisory Services	☐	1	Strategy
☐	2	Project Management	☐	2	Architecture
☐	3	Cyber Security	☐	3	Security and Risk
☐	4	Enterprise Technology	☐	4	Infrastructure
☐	5	Technical Support	☐	5	Business Application Solutions
☐	6	SharePoint Support	☐	6	Salesforce Development
☐	7	Agile Application Delivery	☐	7	Business Intelligence and Analytics
☐	8	Application Development	☐	8	ServiceNow Solutions
☐	9	Business Intelligence and Analytics			
☐	10	ServiceNow Development			

For a Service Category under Service Stream # 1 ONLY, the Bidder should identify one or more Role(s) profiled in this Reference Engagement by placing an "X" in the applicable box.

	#	Role		#	Role
☐	1	IT Executive Strategic Advisor (SC#1)	☐	25	Application Support Specialist (SC#5)
☐	2	Data Strategy Advisor (SC#1)	☐	26	Deskside Technical Support Analyst (SC#5)
☐	3	Project Management Office Lead (SC#2)	☐	27	Service Desk Analyst (SC#5)

☐	4	Project Manager (SC#2)	☐	28	IT Service Management Specialist (SC#5)
☐	5	Project Administrator (SC#2)	☐	29	Infrastructure Operations and Support (SC#5)
☐	6	Security Analyst (SC#3)	☐	30	Technical Writer / Trainer / Courseware (SC#5)
☐	7	Application Security Administrator (SC#3)	☐	31	SharePoint Online Administrator (SC#6)
☐	8	IT Security Architect (SC#3)	☐	32	SharePoint Online Architect (SC#6)
☐	9	Ethical / White Hat Hacker (SC#3)	☐	33	SharePoint Online Developer (SC#6)
☐	10	Azure Security Architect (SC#3)	☐	34	Alteryx Developer (SC#8)
☐	11	Azure Security Administrator (SC#3)	☐	35	Solution Architect (SC#10)
☐	12	Cyber Forensics Specialist (SC#3)	☐	36	Business Analyst (SC#10)
☐	13	Security Engineer (Application / Network) (SC#3)	☐	37	Application Developer (SC#10)
☐	14	SOC Analyst (SC#3)	☐	38	Azure Cloud Application Developer (SC#10)
☐	15	SOC Lead/Manager (SC#3)	☐	39	Quality Assurance (QA)Tester (SC#10)
☐	16	Cloud Security Specialist (SC#3)	☐	40	Business Intelligence Developer (SC#11)
☐	17	Security Administrator (SC#3)	☐	41	Data Architect (SC#11)
☐	18	Governance Risk and Compliance Analyst (SC#3)	☐	42	Data Scientist (SC#11)
☐	19	Storage Admin / Virtualization Architect (SC#4)	☐	43	ServiceNow Developer (SC#12)
☐	20	Systems Architect (SC#4)	☐	44	ServiceNow Implementation Specialist (SC#12)
☐	21	Azure Architect (SC#4)	☐	45	ServiceNow Solution Architect (SC#12)
☐	22	Azure Administrator (SC#4)			
☐	23	Azure Data Base Administrator (SC#4)			
☐	24	Webmaster (SC#4)			

2. Engagement Reference - Client (Company) Contact Information	
Client (Company) Name:	*<<External client in private or public sector>>*
Client (Company) Address:	
Client (Company) Contact Person Name:	
Title:	
Telephone #:	
Email:	

3. Engagement Profile Details			
Engagement/Project Name:			
Engagement Dollar Value:	$*<<must have a dollar value of at least $25,000 CAD OR a statement confirming that the Reference Engagement value was a minimum of $25,000 CAD >>*		
Engagement Start Date: (mm/dd/yyyy)		**Total Level of Effort (Days):** *(7 hours equals 1 working day)*	_____ Days <<must have a duration of at least twenty (20) working days>>
Engagement End Date: (mm/dd/yyyy)			

Part 2 – Service Stream Specific Technical Experience and Expertise - Rated Requirements - Reference Engagements – (Maximum Points – 200 Points - 100 Points per Reference Engagements)

Each Service Category will be evaluated separately. Bidder to complete Appendix "C-2" (Reference Engagement Form).

4. Technical Experience and Expertise - (Maximum Points - 100)

RR4.1 Scope and Type of Services – (Maximum Points – 40)

Bidder should clearly describe in detail the scope and type of services provided, including any similarities/relevance between the client and CDIC's organizations.

The details should clearly demonstrate relevance to the scope of the respective Service Category described in Appendix "A-1" and Appendix "A-2", as applicable, for each Service Category under a Service Stream the Bidder is offering as part of its Proposal.

NOTE: For a Service Category under Service Stream #1 ONLY, the Bidder should also clearly describe relevance to the scope of at least one Role as described in Appendix "A-1".

A4.1 (*Maximum of 500 words)*

RR4.2 Client Management – (Maximum Points – 15)

Bidder should describe in detail how the Engagement was approached by addressing each of the following items:

a) *Understanding and delivery of the client's vision;*
b) *Methodologies and tools used to complete the deliverables;*
c) *Managing client feedback and changes; and.*
d) *Ensuring client engagement and involvement.*

A4.2 (*Maximum of 500 words)*

RR4.3 Knowledge Transfer – (Maximum Points – 15)

Bidder should describe, in detail:

a) *the processes used by the bidder to transfer knowledge to the client upon completion of this Engagement (e.g., reports, training, user manual).*

A4.3 (*Maximum of 500 words)*

RR4.4 Outcome of Engagement – (Maximum Points – 15)

Bidder should describe in detail:

a) the outcome of this Engagement.

A4.4 (*Maximum of 500 words)*

RR4.5 Success Factors – (Maximum Points – 15)

Bidder should describe in detail:

a) the critical success factors and how bidder contributed to achieving the outcome.

A4.5 [(*Maximum of 500 words)*

[END OF APPENDIX "C-2" (REFERENCE ENGAGEMENT FORM)]

Schedule "D"

Financial Offer Requirements and Evaluation

1. **Financial Offer Requirements**

1.1 For greatly clarity, Appendix "D-1" (Financial Offer for Service Stream #1) is **ONLY** required for bidders submitting a proposal for one or more Service Category under Service Stream #1.

The Bidder must submit Financial Offers in Canadian dollars and exclusive of Canadian Goods and Services Tax (GST), Harmonized Sales Tax (HST), and/or provincial sales taxes (PST), as applicable.

1.2 Service Stream #1. Bidder must provide an all-inclusive ceiling hourly rate/price for each Role related to each Service Category under Service Stream #1, as set out in Schedule "A" (Statement of Work), that the bidder will be proposing as part of its Proposal and as outlined in Appendix "D-1", which shall be payable as per Appendix "A" of the Professional Services Agreement, attached to the RFSA as Schedule "F" (Form of Professional Services Agreement).

1.2.1 Rates shall include all labour, materials, photocopies, telephone charges, overhead, profit and all other fees, expenses and costs associated with providing the Services, as set out in Schedule "A" (Statement of Work) and excluding any Pre-approved Expenses and applicable taxes.

1.2.2 The hourly ceiling rates submitted by Bidders will be the ceiling rates applicable for the term of the resulting agreement, with no possibility for an increase. As such, it is the Bidders' responsibility to ensure its rates include amounts for any future adjustments (i.e., inflation).

2. Commercially Reasonable Rates

2.1 Without limiting Section 11, CDIC's Reserved Rights, of the RFSA, where a Bidder submits rates that are considered to be, in CDIC's sole and absolute discretion, commercially unreasonable, CDIC may deem the rates non-compliant and reject the Financial Offer.

3. Non-Resident Bidders

3.1 Any Bidder who is a non-resident of Canada for tax purposes shall clearly state this fact in its Financial Offer; otherwise, the Bidder shall be deemed to have represented that it is a resident of Canada for tax purposes.

4. Mathematical Errors

4.1 In assessing Financial Offers, subject to Section 11, CDIC's Reserved Rights, of the RFSA, any Bidder affected by mathematical errors identified by CDIC may be contacted for clarification.

5. Pricing Tables/Forms

5.1 Bidders submitting a Proposal under one or more Service Category under Service Stream #1 should provide all applicable rates by fully completing Appendix "D-2" (Financial Offer for Service Stream #1). Bidders that do not provide Appendix "D-2" (Financial Offer for Service Stream #1) as part of their Financial Offer will not be given further consideration to qualify for a Role/Service Category under that Service Stream.

[END OF SCHEDULE "D" (FINANCIAL OFFER REQUIREMENTS AND EVALUATION)]

Appendix "D-1"

Financial Offer Submission Form

INSTRUCTIONS TO BIDDERS: The Financial Offer Submission Form shall be completed and accompanied by Appendix "D-2" (Financial Offer for Service Stream #1), as applicable.

FINANCIAL OFFER

LEGAL NAME OF BIDDER: _____

ADDRESS: _____

CONTACT NAME: _____

TELEPHONE: _____

EMAIL: _____

SOLICITATION NUMBER: **RFSA 2023-3941**

TITLE: **Information Technology Staff Augmentation and Project Delivery Services**

1. The undersigned bidder (hereinafter referred to as the "**Bidder**") hereby offers the Canada Deposit Insurance Corporation ("CDIC") to perform and complete the work at the place, in the manner set out in accordance with the documents specified in the RFSA and any additional documents or information submitted as part of its Technical Offer and at the prices specified herein.

2. The Bidder has submitted its pricing in accordance with the instructions in the RFSA and in Schedule "D" (Financial Offer Requirements and Evaluation) in particular. The Bidder confirms that the pricing information provided is accurate. The Bidder acknowledges that any inaccurate, misleading or incomplete information, including withdrawn or altered pricing, could adversely impact the acceptance or ranking of its proposal or its eligibility for future work.

3. Appropriate Law

   This RFSA and any Agreement and subsequent purchase order authorized as a result of this RFSA shall be governed by and construed in accordance with the laws in force in the Province of Ontario, Canada.

4. Place of Residence Information

   Bidder **Resident** of Canada for Canadian tax purposes ☐

   Bidder **Non-resident** of Canada for Canadian tax purposes ☐

   If not specified, the Bidder will be deemed to represent and warrant that it is a resident of Canada for Canadian tax purposes.

By signing this Form, the Bidder represents that the above information is accurate.

Signature	Date
Print Name	Title

I have the authority to bind the Bidder.

OFFERS WHICH DO NOT CONTAIN THE REQUESTED DOCUMENTATION MAY BE DEEMED NON-COMPLIANT.

[END OF APPENDIX "D-1" (FINANCIAL OFFER SUBMISSION FORM)]

Appendix "D-2"

Financial Offer for Service Stream #1

INSTRUCTIONS TO BIDDERS: The bidder must not alter the format of the table below in any way, other than to remove highlighted text and add hard returns to provide responses. Columns and rows are not to be added or deleted.

Bidder should provide all-inclusive hourly ceiling rates for the applicable Roles they are offering for the categories listed for Service Stream # 1.

For clarity, Rates are requested for information purposes only and will not be evaluated as part of this RFSA, however, will be the maximum ceiling rates under any resulting agreement for the duration of the term. Rates for each Role are not required. However, only Bidders that have provided a rate for a particular Role may be qualified for that Role and will be eligible to receive a Service Request.

Role #	Service Category #1 - Advisory Services	Level 1	Level 2	Level 3
1	IT Executive Strategic Advisor	$	$	$
2	Data Strategy Advisor	$	$	$

Role #	Service Category #2 - Project Management	Level 1	Level 2	Level 3
3	Project Management Office Lead	$	$	$
4	Project Manager	$	$	$
5	Project Administrator / Coordinator	$	$	$

Role #	Service Category #3 - Cyber security	Level 1	Level 2	Level 3
6	Security Analyst	$	$	$
7	Application Security Administrator	$	$	$
8	IT Security Architect	$	$	$
9	Ethical / White Hat Hacker (or Penetration Tester)	$	$	$
10	Azure Security Architect	$	$	$
11	Azure Security Administrator	$	$	$
12	Cyber Forensics Specialist	$	$	$
13	Security Engineer (Application/Network)	$	$	$
14	SOC Analyst	$	$	$
15	SOC Lead/Manager	$	$	$
16	Cloud Security Specialist	$	$	$
17	Security Administrator	$	$	$
18	Governance Risk and Compliance Analyst	$	$	$

Role #	Service Category #4 - Enterprise Technology	Level 1	Level 2	Level 3
19	Storage Administrator / Virtualization Architect	$	$	$
20	Systems Architect (network, data, applications)	$	$	$
21	Azure Architect	$	$	$
22	Azure Administrator	$	$	$
23	Azure Data Base Administrator	$	$	$
24	Webmaster	$	$	$

Role #	Service Category #5 - Technical Support	Level 1	Level 2	Level 3
25	Application Support Specialist	$	$	$
26	Deskside Technical Support Analyst	$	$	$
27	Service Desk Analyst	$	$	$
28	IT Service Management Specialist	$	$	$
29	Infrastructure Operations and Support	$	$	$

30	Technical Writer / Trainer / Courseware Author (Developer)	$	$	$

Role #	Service Category #6 – SharePoint Support	Level 1	Level 2	Level 3
31	SharePoint Online Administrator	$	$	$
32	SharePoint Online Architect	$	$	$
33	SharePoint Online Developer	$	$	$

Role #	Service Category #7 – Alteryx Support	Level 1	Level 2	Level 3
34	Alteryx Developer	$	$	$

Role #	Service Category #8 - Application Development	Level 1	Level 2	Level 3
35	Solution Architect	$	$	$
36	Business Analyst	$	$	$
37	Application Developer	$	$	$
38	Azure Cloud Application Developer	$	$	$
39	Quality Assurance (QA)Tester	$	$	$

Role #	Service Category #9 - Business Intelligence and Analytics	Level 1	Level 2	Level 3
40	Business Intelligence Developer	$	$	$
41	Data Architect	$	$	$
42	Data Scientist	$	$	$

Role #	Service Category #10 – ServiceNow Development	Level 1	Level 2	Level 3
43	ServiceNow Developer	$	$	$
44	ServiceNow Implementation Specialist	$	$	$
45	ServiceNow Solution Architect	$	$	$

[END OF <u>APPENDIX "D-2"</u> (FINANCIAL OFFER FOR SERVICE STREAM # 1)]

Schedule "E"

Required Forms

The following is a list of required forms which must be included in the bidder's Proposal as applicable.

Appendix	Description and Requirement
Schedule "C"	Technical Offer Submission Form
Appendix "C-1"	Technical Offer (*One (1) per Proposal*)
Appendix "C-2"	Reference Engagement Form *(Two (2) per Service Stream)*
Appendix "D-1"	Financial Offer Submission Form
Appendix "D-2"	Financial Offer for Service Stream # 1 (*as applicable*)

[END OF SCHEDULE "E" (REQUIRED FORMS)]

Schedule "F"

Form of Professional Services Agreement

Attached is the Professional Services Agreement ("PSA") for this RFSA.

It is CDIC's intent to execute all agreements awarded under this RFSA based on this PSA to facilitate contract management activities, notwithstanding any deviations previously agreed to by CDIC in other agreements. Within the PSA are highlighted provisions that cover issues that CDIC will require be addressed in the final form of agreement. Bidder may request adjustments to the standard form, however, CDIC may refuse to consider any bidder's request, in its sole and absolute discretion.

PROFESSIONAL SERVICES AGREEMENT

THIS AGREEMENT is made as of the Execution Date

BETWEEN:

CANADA DEPOSIT INSURANCE CORPORATION,
a federal crown corporation established by an Act of Parliament, with a head office located at 50 O'Connor Street, Ottawa, Ontario, K1P 6L2
("**CDIC**")

AND:

[insert name of corporation or partnership],
a corporation incorporated under the laws of <*>, with a registered office located at [ENTER COMPLETE MAILING ADDRESS OF THE ENTITY]
or
a (**limited liability**) partnership established pursuant to the laws of <*>, with a registered office located at [ENTER COMPLETE MAILING ADDRESS OF THE ENTITY]
("**Supplier**").

BACKGROUND

A. Following a request-for-supply-arrangements process for information technology staff augmentation and project delivery services (the "**RFSA**"), CDIC has selected the Supplier to provide the Services on a standby/as-needed basis as set out in Appendix A to this Agreement. CDIC makes no guarantee as to the value or volume of work, if any to be assigned to any Supplier.

B. The Supplier is qualified to provide the Services and agrees to provide the Services in accordance with the terms and conditions of this Agreement.

IN CONSIDERATION of the Background, the mutual covenants set out herein, and other good and valuable consideration (the receipt and sufficiency of which are hereby acknowledged), the Parties agree as follows:

ARTICLE 1
DEFINITIONS AND INTERPRETATION

1.1 Definitions. Whenever used in this Agreement, the following words and terms shall have the meanings set out below:

"**Acceptance**", "**Accepts**", "**Accepted**" or "**Acceptable**" means the confirmation in writing by the Designated Officer that CDIC is satisfied with the quality of the Services and/or Work Product provided;

"**Agreement**" means this Professional Services Agreement and includes the appendices and any schedules attached hereto, as such may be amended from time to time by written agreement of the Parties hereto;

"**Assigned Person**" means any person employed or engaged by the Supplier who is (i) assigned by the Supplier to perform the Services and is listed in the particular Task Authorization, or (ii) who is assigned by the Supplier to perform the Services as an alternate, pursuant to Section 6.5;

"**Business Day**" means a day, other than a Saturday, Sunday or a statutory or civic holiday in the City of Ottawa, Province of Ontario, Canada;

"**Claim**" means any claim, demand, action, assessment or reassessment, suit, cause of action, damage, loss, charge, judgment, debt, costs, liability or expense, including taxes, interest and penalties imposed by law and the reasonable professional fees and all costs incurred in investigating or pursuing, defending or settling any of the foregoing or any proceeding relating to any of the foregoing;

"**Commencement Date**" means the date set out in Appendix A on which the Supplier shall begin to provide the Services;

"**Completion Date**" means the date set out in Appendix A on which the Supplier shall cease to provide the Services;

"**Confidential Information**" has the meaning attributed thereto in Appendix C;

"**Designated Officer**" means the individual set out in Appendix A who represents CDIC, or such other person as may be designated by CDIC from time to time;

"**Disbursements**" means the reasonable fees, expenses, costs or charges, from other parties that are incurred by the Supplier for the purpose of performing the Services including all applicable taxes thereon, but do not include Pre-approved Expenses;

"**Execution Date**" means the latest date this Agreement, is signed by the Parties as indicated on the signature page;

"**Fee**" or "**Fees**" means an amount agreed to be paid to the Supplier for the provision of any part of the Services as set out in Appendix A;

"**Force Majeure Event**" has the meaning provided in Article 13.

"**GST/HST/PST**" means all taxes exigible under Part IX of the *Excise Tax Act*;

"**Information**" means all information provided to the Supplier and any Assigned Person, regardless of form or medium, whether reproducible or not, and includes any facts, data, hypotheses, analyses, projections, assumptions, or opinions;

"**Intellectual Property Rights**" means any rights provided under: (i) patent law; (ii) copyright law (including moral rights); (iii) trade-mark law; (iv) design patent or industrial design law; (v) semi-conductor chip or mask work law; or (vi) any other statutory provision or common law principle applicable to this Agreement, including trade secret law, which may provide a right in either hardware, software, documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how generally, or the expression or use of such hardware, software, documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how; or any rights provided under any applications, registrations, licenses, sub-licenses, franchises, agreements or any other evidence of a right in any of the foregoing;

"**Non-Compliant Jurisdiction**" means any jurisdiction whose laws conflict with or impede the application of the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*, either expressly or through subsequent application. This includes the United States of America;

"**Parties**" means CDIC and the Supplier, and "**Party**" means either one of them;

"**person**" includes an individual, a corporation, a general or limited partnership, a joint venture, a trust, an unincorporated organization, the Crown or a federal, provincial, national, state or municipal government or any agency or instrumentality of the Crown or a government or any entity recognized by law;

"**Personal Information**" means Confidential Information about an identifiable individual;

"**Pre-approved Expenses**" mean the reasonable out-of-town travel, accommodation and living expenses, including all applicable taxes thereon, that are expected to be incurred by the Supplier for the purpose of performing the Services and that are approved by CDIC's Designated Officer prior to actually being incurred;

"**RFSA**" means the Request for Supply Arrangements dated August 16, 2023, for IT staff augmentation services and project delivery services reference number RFSA # 2023-3941 issued by CDIC and any addenda to it;

"**Services**" means the tasks or activities required to be performed by the Supplier as set out in Appendix A and any services ancillary thereto;

"**Service Request**" means a document issued by CDIC to a Supplier, that includes instructions and applicable CDIC service requirements, which may result in a Task Authorization;

"**Task Authorization**" means the authorization issued by CDIC, following the receipt of a Supplier's response to a Service Request, authorizing services to commence;

"**Total Fee**" means the total amount payable to the Supplier for the provision of the Services as indicated in each Task Authorization issued by CDIC; and

"**Work Product**" means all materials, inventions and other deliverables that the Supplier may develop for CDIC in the course of providing the Services, whether alone or jointly with others, including all research, reports, correspondence, memoranda, notes, source code, object code, executable code, technical documentation, user documentation, custom software and all information generated by the Supplier specifically for CDIC in any reproducible medium in connection with the provision of the Services.

1.2 Certain Rules of Interpretation. In this Agreement,

(a) **Time** - the Supplier will use all reasonable efforts to complete within any agreed upon time frame the performance of the Services. However, the Supplier will not be liable for failures or delays in performance that arise from causes beyond its control;

(b) **Currency** - unless otherwise specified, all references to monetary amounts in this Agreement are to lawful currency of Canada;

(c) **Headings** - descriptive headings of Articles and Sections are inserted solely for convenience of reference and are not intended as complete or accurate descriptions of the content of such Articles or Sections and as such, shall not affect the construction or interpretation of this Agreement;

(d) **Singular, etc**. - words expressed in the singular include the plural and vice-versa and words in one gender include all genders;

(e) **Consent** - whenever a provision of this Agreement requires an approval or consent by a Party to this Agreement and notification of such approval or consent is not delivered within the applicable time, then, unless otherwise specified, the Party whose consent or approval is required shall be conclusively deemed to have withheld its approval or consent;

(f) **Calculation of Time** - unless otherwise specified, time periods within or following which any payment is to be made or act is to be done shall be calculated by excluding the day on which the period commences and including the day on which the period ends;

(g) **Business Day** - whenever any payment is to be made or action to be taken under this Agreement is required to be made or taken on a day other than a Business Day, such payment shall be made or action taken on the next Business Day following such day;

(h) **Inclusion** - where the words "including" or "includes" appear in this Agreement, they mean "including without limitation" or "includes without limitation" respectively;

(i) **References** - the words "herein", "hereof", "hereby" and "hereunder" and similar expressions refer to this Agreement as a whole and not to any particular portion of it and references to an Article, Section or subsection refer to the applicable Article, Section or subsection of this Agreement; and

(j) **No Strict Construction** – the language used in this Agreement is the language chosen to express the mutual intent of the Parties, and no rule of strict construction will be applied against either of the Parties.

1.3 **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein. The rights and obligations under this Agreement shall not be governed by the *United Nations Convention on Contracts for the International Sale of Goods* or any local implementing legislation, the application of which is expressly excluded.

1.4 **Appendices**. The appendices to this Agreement listed below include additional terms which form part of this Agreement:

Appendix	**Description**
A	Services and Fees
B	Service Stream(s), Service Categories/Roles
C	Confidentiality, Privacy, Conflict of Interest and Security
D	Service Request and Task Authorization Form

ARTICLE 2
AGREEMENT FOR SERVICE

2.1 The Supplier is hereby engaged by CDIC as an independent contractor on a non-exclusive basis for the sole purpose of undertaking and delivering the Services set out in Appendix A, any Task Authorization, and any applicable Work Product for the term set out therein, and in accordance with this Agreement.

2.2 CDIC makes no guarantee as to the volume or value of work to be assigned, if any, to the Supplier and the Supplier acknowledges same.

2.3 Subject to the conflict of interest provisions contained in Appendix C, CDIC acknowledges that, during the term of this Agreement, the Supplier and any Assigned Person may provide services to other persons (including member institutions of CDIC or any parent or subsidiary corporations or affiliates thereof).

2.4 The Supplier is responsible for the delivery of all filings required in relation to, and the payment of: all taxes, levies, premiums or payments assessed, levied or charged against the Supplier, including any GST/HST/PST, income tax, local tax, workplace safety and insurance premiums, Canada Pension Plan or Quebec Pension Plan premiums, Employment Insurance premiums and Ontario Health Insurance Plan premiums or levies or other contributions as required by all laws applicable to the Supplier or to any Assigned Person (all collectively, the "**filings and deductions**"). In addition to any other indemnifications contained in this Agreement, the Supplier agrees to indemnify and save harmless CDIC, its employees, agents, officers and directors from any Claims arising as a result of or in relation to:

(a) the Supplier's failure, omission or refusal to deliver or remit any filings and deductions to the appropriate federal, provincial or municipal government entity, agency or collecting body, as required by law; or,

(b) a determination by any federal, provincial or municipal government entity, agency or collecting body that (notwithstanding the express and mutual intention of the Parties,) the relationship between CDIC and any of the Supplier or any Assigned Person, is not an independent contractor relationship.

ARTICLE 3
LIMITATION OF AUTHORITY

3.1 The Supplier shall have no authority to enter into any contract, commitment or obligation of any kind whatsoever on behalf of CDIC unless the Supplier receives prior written authorization from CDIC.

3.2 Neither the Supplier nor any Assigned Person shall, at any time, be deemed to be an employee, servant or agent of CDIC or of Her Majesty in Right of Canada, for any purpose whatsoever.

ARTICLE 4
CONFIDENTIALITY AND CONFLICT OF INTEREST AND USE OF PERSONAL AND CONFIDENTIAL INFORMATION

4.1 The Supplier agrees to be bound by the terms set out in this Article 4 and in the attached Appendix C entitled "Confidentiality, Privacy Conflict of Interest and Security".

4.2 The Supplier agrees that prior to allowing any Assigned Person to perform the Services, it shall require that Assigned Person to read and agree to abide by the terms of the attached Appendix C entitled "Confidentiality, Privacy, Conflict of Interest and Security".

4.3 Except as set out in Appendix A, the Supplier represents and warrants that:

(a) The Supplier only carries on business in Canada;

(b) The Supplier does not have a parent, subsidiary or other related company that operates in a Non-Compliant Jurisdiction;

(c) The Supplier does not subcontract or outsource data processing or storage to any third party carrying on business in a Non-Compliant Jurisdiction; and

(d) The Supplier's employees are bound by written confidentiality agreements or binding confidentiality policies.

4.4 The Supplier agrees that:

(a) CDIC shall retain custody and control of any Confidential Information and Personal Information transferred, collected, created, obtained, maintained or otherwise held by the Supplier for the purposes of this Agreement, and all Confidential Information and Personal Information must be returned to CDIC upon request;

(b) Except as set out in Appendix A, the Supplier shall not transfer Personal Information to any entity or person carrying on business in a Non-Compliant Jurisdiction for any purpose unless approved by CDIC in writing. Confidential Information may be disclosed to third parties that provide data processing, storage and similar services to

the Supplier and may correspondingly be used, processed and stored outside Canada by the Supplier and such third-party service providers. The Supplier is responsible to CDIC for causing such third-party service providers to comply with the obligations of confidentiality set out in this Agreement;

(c) CDIC shall have the right to review from time to time the measures and practices adopted by the Supplier to perform its obligations under this Agreement. This right of review includes the right to be escorted, in accordance with the Supplier's security rules and heavily restricted to certain areas of the Supplier's premises on reasonable written notice to the Supplier to attend the Supplier's premises on reasonable written notice to the Supplier to review such measures and practices and the right to audit the Supplier's relevant records and otherwise verify audit trails for data access, modification or disclosure. The Supplier shall provide full cooperation in connection with any such review. To the extent that such review causes the Supplier to incur reasonable third-party expenses, such expenses shall be reimbursed by CDIC;

(d) The Supplier shall implement sufficient audit trail requirements to record access to Confidential Information and any attempted access thereto and any modification or disclosure of Confidential Information; and

(e) The Supplier shall include the above representations, warranties and terms in any agreement with a third party respecting the transfer of Confidential Information or Personal Information, *mutatis mutandis*.

4.5 If the Supplier learns of any actual or reasonably suspected access, use, destruction, alteration or disclosure of Confidential Information or Personal Information that is not permitted by this Agreement or otherwise approved by CDIC in writing (including any loss or theft of Confidential Information or Personal Information) (collectively, a "**Data Breach**"), Supplier shall promptly notify CDIC in writing of the particulars of such Data Breach (unless such notice is prohibited by applicable law). The Supplier shall thereafter contain and investigate the Data Breach and fully cooperate with CDIC in resolving the Data Breach.

4.6 In the event of a change in status or ownership of a parent company or of the Supplier that may result in a change of custody or control of data being held and/or processed by the Supplier, the Supplier shall promptly notify CDIC. Following such notification, CDIC reserves the right to immediately terminate this Agreement or seek amendments thereto.

4.7 In the event of a change in the operations of the Supplier, such as acquiring or creating an entity in a Non-Compliant Jurisdiction that shall have access to CDIC Information, the Supplier shall promptly notify CDIC. Following such notification, CDIC reserves the right to immediately terminate this Agreement or seek amendments thereto.

ARTICLE 5
CDIC'S RESPONSIBILITIES

5.1 If and when necessary, CDIC shall provide the Supplier with limited access, as required, to its offices and personnel at 50 O'Connor Street, Ottawa, Ontario and 79 Wellington Street West, Suite 1200, Toronto, Ontario (collectively, the "**Premises**") to facilitate the provision of the Services. The Supplier agrees to abide by the requirements of CDIC and the Designated

Officer with respect to security, timing and manner and method of access, occupancy and egress from the Premises, as those requirements may change from time to time. The Supplier further agrees to abide by any rules regarding access, occupancy and egress imposed by the landlord of the Premises.

5.2 The Designated Officer, or other representative of CDIC, as may be appropriate, shall provide the Supplier with the Information and Confidential Information that is required for the provision of the Services.

5.3 CDIC acknowledges that the provision of the Services may require the Designated Officer and other CDIC personnel to be available for meetings with the Supplier and to respond promptly to the inquiries of the Supplier. CDIC shall use reasonable efforts to accommodate same without disrupting its operations.

5.4 The Supplier shall consult with the Designated Officer from time to time, regarding the provision of the Services. The Designated Officer may provide the Supplier with a schedule for the completion of the Services (the "**Schedule**").

5.5 CDIC may, at its own discretion, periodically or from time to time, advise the Supplier as to whether the provision of Services by the Supplier is Acceptable. CDIC shall have the right to require the Supplier to correct or replace any Services and Work Product that are deemed by CDIC not to be Acceptable, at the Supplier's own expense. CDIC shall inform the Supplier of the reasons for any such non-Acceptance of the Services or Work Product as the case may be.

5.6 CDIC or its representatives may, at any time during the term of this Agreement or within one (1) year of the expiration or termination of this Agreement, upon reasonable prior written notice to Supplier, and during the regular business hours of the Supplier conduct an audit of the books, accounts, records, and data of the Supplier relating to the performance of the Services and of all expenditures or commitments made by the Supplier in connection therewith. The Supplier shall not, without the prior written consent of CDIC, dispose of any books, accounts or records that relate to the performance of the Services until the later of: (i) the expiration of one (1) year after the final payment is made under this Agreement; or (ii) the settlement of all outstanding claims and disputes between the Parties. The Supplier shall provide CDIC with access to all books, accounts, and records related to the performance of the Services and shall reasonably co-operate with CDIC in respect of any audit that is conducted.

ARTICLE 6
SUPPLIER'S RESPONSIBILITIES

6.1 The Supplier shall provide the Services promptly, efficiently, in accordance with reasonable standards of quality acceptable to CDIC, in consultation with the Designated Officer, in conformity with the Schedule established by the Designated Officer, if any, and with the terms and provisions of this Agreement.

6.2 The Supplier shall commence the provision of the Services on the Commencement Date and shall provide the Services until the earlier of the Completion Date or the date on which the Services are completed by the Supplier and Accepted by the Designated Officer.

6.3 The Supplier shall make periodic written reports, as requested by the Designated Officer, outlining the progress made by the Supplier in providing the Services.

6.4 CDIC is required to notify individuals in connection with the collection of Personal Information by CDIC. The Supplier agrees that prior to providing any Personal Information about an Assigned Person to CDIC, or prior to allowing an Assigned Person to perform the Services, as applicable, the Supplier shall either (a) provide the Assigned Person with CDIC's privacy notice (a copy of which is at *http://www.cdic.ca/en/about-cdic/policies-reports/atip/Pages/Privacy.aspx*), or (b) refer the Assigned Person to the webpage where the privacy notice is posted, and require the Assigned Person to read the privacy notice.

6.5 The Supplier shall ensure that the Services are only provided by the Assigned Persons listed in the Task Authorization outlined in the Service Request and Task Authorization Form and that such Assigned Persons are available to perform the Services in accordance with the Schedule established by the Designated Officer, if any. Should such Assigned Person be unavailable to provide the Services, the Supplier may, with CDIC's prior written consent, acting reasonably, assign an alternate Assigned Person who has a comparable level of skill, ability and qualifications to provide the Services. Other amendments to the list of Assigned Persons in the Task Authorization may be made with the written consent of CDIC.

6.6 CDIC shall have access at all reasonable times to the books, accounts, records, data, Work Product and other information in the Supplier's and any Assigned Person's possession and control in connection with the provision of the Services.

6.7 On termination for any reason other than breach by CDIC, to the extent that it may exist, in whole or in part, the Supplier shall deliver to CDIC, or such person as CDIC may designate, the Work Product and knowledge that is required by CDIC to complete the provision of the Services or that will allow CDIC to utilize the Services or Work Product on an ongoing basis.

6.8 The Supplier acknowledges and agrees that CDIC may require the Supplier to require any Assigned Person, to act in conformity with any existing or future policies, standards, guidelines and procedures of CDIC as may become appropriate in CDIC's discretion, at all times during the provision of the Services, including:

(a) where the Services involve Personal Information or other "Protected Information", as that term is defined in CDIC's *Information Classification Standard*, the Supplier will adhere to CDIC's *Corporate Security Policy;*

(b) where the Services involve travel and related living expenses, the Supplier will adhere to CDIC's *Travel, Hospitality, Conferences and Events Policy*; and

(c) where any Assigned Person will be performing Services at CDIC's Premises on a regular basis, to require any Assigned Person to review and act in conformity with: (i) the Guidelines for Contractor/Consultants' Personnel/Agency Personnel (the "**Guidelines**") and (ii) *Harassment and Violence Prevention Policy* prior to or on the date such Assigned Person commences performing the Services; and CDIC's *Vaccination Policy for Third-Parties.*

6.9 The Supplier shall be responsible for ensuring that each Assigned Person complies with all of the terms of this Agreement and shall be responsible for any non-compliance in any way attributable to any Assigned Person or other person for whom the Supplier is responsible. For greater certainty, in no event shall Supplier be relieved of any of its obligations as a result of its use of subcontractors and under no circumstances shall CDIC be required to assume any liability or obligation or pay any amount greater than what would be assumed or paid if Supplier had completed the Services himself.

6.10 If CDIC determines that any Assigned Person is unsatisfactory, CDIC may notify Supplier of its determination, indicating the reasons therefore, in which event Supplier shall promptly, as directed by CDIC, take all necessary actions including by remedying the performance, or conduct of such Assigned Person, replacing such Assigned Person by another third party, or cease such subcontracting, in a manner satisfactory to CDIC.

6.11 In the event Supplier does not (or expects that it may not be able to) perform Services or deliver the Work Product as required pursuant to this Agreement or any Service Request (including in accordance with any Schedule), Supplier shall promptly advise CDIC and provide all relevant information relating to such inability, including by providing up-to-date information on available quantities, schedule, root causes, workaround plans, and any other reasonable information requested by CDIC.

6.12 If any Force Majeure Event affecting Supplier prevents, hinders, or delays performance of the Services or provision of the Work Product, CDIC may, in its sole discretion, request that Supplier provide CDIC with substitute Work Product and/or Services or undertake to (or CDIC may itself) procure such Services and/or Work Product from an alternate source. CDIC is entitled to approve all replacement Services and/or Work Product (which shall in any event conform to the minimum requirements of the Agreement).

ARTICLE 7
REPRESENTATIONS AND WARRANTIES

7.1 **By Supplier**: Supplier represents, warrants and covenants (and acknowledges that CDIC is relying on), as follows:

(a) The Supplier represents and warrants that it is validly incorporated under the laws of <*> and that it has the power and authority to enter into this Agreement.

(b) The Supplier represents and warrants that the Supplier has and shall maintain in good standing, all licenses, registrations, permits and other authorizations necessary to perform its obligations under this Agreement and that Supplier and each Assigned Person has the necessary resources, competence and qualifications, including knowledge, skill and experience to provide the Services.

(c) The execution and performance of this Agreement by Supplier shall not violate any laws and shall not breach any agreement, license, covenant, duty, court order, judgment, or decree to which Supplier is a party or by which it is bound.

(d) All information furnished by Supplier in connection with the retention (including the continued retention) of Supplier pursuant to this Agreement, fairly and accurately

represents, as applicable, the Services and/or Work Product as well as the business, properties, financial condition, and results of operations of Supplier.

(e) There is no actual, pending or anticipated civil or criminal litigation in any judicial or arbitral forum: (i) that involves Supplier or any of its affiliates or subcontractors, or (ii) otherwise to the knowledge of Supplier, in each case that may adversely affect Supplier's ability to perform its obligations under this Agreement.

(f) Neither Supplier nor any employee of either, has or shall have any contractual, financial, business, or other interest, direct or indirect, that may conflict in any manner with Supplier's performance of its duties and responsibilities to CDIC under this Agreement or otherwise create an appearance of impropriety with respect to the retention of Supplier pursuant to this Agreement.

(g) The Services and/or Work Product: (i) shall conform to all requirements and specifications set forth in this Agreement, (ii) shall be free from defect, whether latent or patent, in workmanship or design, (iii) shall be suitable, merchantable, and fit for CDIC's particular purpose, (iv) shall comply with all applicable laws, and (v) shall not infringe any third party Intellectual Property Rights, including any third party rights relating to patents, industrial designs, trademarks, trade names, service marks, copyrights, trade secrets or Confidential Information.

(h) If the Supplier is required to correct or replace the Services or Work Product or any portion thereof, it shall be at no cost to CDIC, and any Services or Work Product corrected or replaced by the Supplier shall be subject to all the provisions of this Agreement to the same extent as the Services or Work Product as initially performed

(i) Supplier shall use adequate numbers of qualified individuals with suitable training, education, experience, and skill to perform this Agreement. The Services shall be rendered with promptness and diligence and will be executed in a workmanlike manner, in accordance with the practices and professional standards used in well-managed operations performing the obligations of Supplier pursuant to this Agreement.

(j) Supplier is not aware of any past or present, actual, threatened or suspected action taken through the use of Supplier's systems that have resulted or may result in any unauthorized access or use by a third party or misuse, damage or destruction.

7.2 **By each of Supplier and CDIC**: Each of Supplier and CDIC represents, warrants, and covenants to the other and acknowledges that the other is relying thereon, as follows:

(a) It is a Person duly organized and validly existing under the laws of its jurisdiction of organization or incorporation.

(b) It has full legal power and authority to execute and deliver this Agreement, to perform its obligations thereunder and carry out the transactions contemplated thereby. The execution, delivery and performance of this Agreement has been and shall be duly and validly authorized.

(c) The Agreement constitutes valid and binding obligations of such Party, enforceable against it in accordance with its terms subject to the following qualifications:

(i) specific performance, injunction and other equitable remedies are discretionary and, in particular, may not be available where damages are considered an adequate remedy; and

(ii) enforcement may be limited by bankruptcy, insolvency, liquidation, reorganization, reconstruction and other similar laws generally affecting the enforceability of creditors' rights.

(d) It shall perform its obligations under this Agreement in a manner that at least comply with the requirements of all applicable governmental authorities.

(e) It has not violated and will not violate any applicable laws or regulations regarding the offering of unlawful inducements in connection with this Agreement.

ARTICLE 8
OWNERSHIP OF INTELLECTUAL PROPERTY

8.1 The Supplier agrees that prior to allowing any Assigned Person to perform the Services, it shall require that Assigned Person to read and agree to abide by the terms of this Article 8.

8.2 If, during the course of providing Services to CDIC, the Supplier develops any work for CDIC that is protected by copyright, the Supplier hereby waives unconditionally any moral rights it may have in such work and shall require each Assigned Person to waive unconditionally any moral rights in such work upon applicable payment by CDIC to Supplier.

8.3 The Supplier shall not use or disclose any Work Product or other materials embodying any of CDIC's Intellectual Property Rights provided by CDIC or developed for CDIC except in the course of providing the Services or as expressly authorized by CDIC in writing.

8.4 The Supplier shall not make any unauthorized use of any trade secrets or Intellectual Property Rights of a third party during the course of providing Services to CDIC.

8.5 The Supplier shall not make any unauthorized use of CDIC's property including its computer systems, communications networks, databases or files, and shall adhere to all CDIC policies regarding the use of such computer systems, communication networks, databases or files provided that such policies have been provided to Supplier in writing prior to execution of this Agreement.

8.6 The Supplier shall only use software authorized by CDIC on CDIC equipment.

8.7 The Supplier acknowledges and agrees that it shall be held liable for any breach or any damages resulting from any violations of the terms of this Article 7 that are caused by the Supplier or that are attributable in any way to an Assigned Person.

8.8 All Work Product first created for CDIC shall be the exclusive property of CDIC and the Supplier shall have no right, title or interest in any such Intellectual Property Rights. At the request and expense of CDIC, the Supplier shall do all acts necessary and sign all documentation necessary in order to assign all rights in the Intellectual Property Rights to

CDIC and to enable CDIC to register patents, copyrights, trade-marks, mask works, industrial designs and such other protections as CDIC deems advisable anywhere in the world.

8.6 The Supplier agrees to provide all reasonable assistance to CDIC in the prosecution of any patent application, copyright registration or trade-mark application or the protection of any Intellectual Property Rights. The Supplier agrees to execute any documentation necessary to assist with any such prosecution or to effect any such application or registration upon the request of CDIC, whether such request is made during the term of this Agreement or after the expiration or termination of this Agreement for any reason whatsoever.

ARTICLE 9
FEES AND BILLING PROCEDURES

9.1 The Total Fee payable under this Agreement is set out in each Task Authorization. The Supplier shall have no right to demand any additional Fees other than as set out in each Task Authorization, either before, during or after the completion of provision of the Services.

9.2 In accordance with the terms of Appendix A, the Supplier shall deliver a written request for payment in the form of an invoice for services rendered to CDIC (the "**Invoice**").

9.3 The Invoice shall be accompanied by supporting documentation confirming the amount and particulars of any Disbursements or Pre-approved Expenses incurred by the Supplier in providing the Services and shall specify the following information, as applicable:

(a) a detailed suitable description of the Services provided in relation to the Fees billed by the Supplier, including timesheets;

(b) the amount owing in accordance with the Fees set out in Appendix A;

(c) the amount of GST/HST/PST thereon;

(d) the amount of any Disbursements and Pre-approved Expenses; and

(e) such other information as CDIC may reasonably require.

The Supplier agrees that failure to include all supporting documentation with the Invoice and/or failure to provide any or all of the foregoing information as part of the Invoice may result in a delay of payment to the Supplier.

9.4 Within thirty (30) days of receiving an Invoice, CDIC shall verify the amounts stipulated in the Invoice and subject to Section 9.1 hereof, shall pay to the Supplier the full amount of the Invoice. CDIC shall advise the Supplier of the details of any objection it may have to the form, content or amount of the Invoice within fifteen (15) days of receipt of the Invoice, and the above-noted thirty (30) day period shall commence to run after receipt by

CDIC of a revised Invoice. The Parties will use the dispute resolution procedure set out in Article 12 to resolve all Invoice disputes in good faith. The Supplier will continue performing the Services in accordance with this Agreement pending resolution of an Invoice dispute.

9.5 Subject to Section 9.3 hereof, upon termination of this Agreement by CDIC, the Supplier shall, within fifteen (15) days after the effective date of such termination, deliver a final Invoice to CDIC in the form specified above setting out the Fees, GST/HST/PST, Disbursements, and Pre-approved Expenses charged or incurred by the Supplier from the date of the previous Invoice to the effective date of termination and CDIC shall pay the Invoice in accordance with this Article 9. The Supplier shall not be entitled to payment for any amount on account of Fees, GST/HST/PST, Disbursements or Pre-approved Expenses that are either charged or incurred by the Supplier following the effective date of termination of this Agreement.

[For Non-Resident Suppliers:

9.6 Unless otherwise specified herein, any and all taxes, duties, fees, levies and other impositions imposed by the laws of a non-Canadian jurisdiction, including without limitation federal excise tax, state or local sales or use tax, value-added tax, income tax, and any other foreign tax whatsoever, are included in the Total Fee for each particular Task Authorization.

9.7 Where any amounts payable by CDIC under the Agreement are subject to any Canadian federal or provincial deduction, withholding or similar tax, CDIC shall deduct or withhold the necessary amount it is required to deduct or withhold from the amounts to be paid to the Supplier under the Agreement, unless the Supplier provides proper documentation from the competent Canadian federal or provincial governmental authority relieving CDIC of its withholding obligations prior to payment being made. The Supplier is solely responsible, at all times, for obtaining its own professional advice regarding any Canadian federal or provincial deduction and withholding or similar tax.]

ARTICLE 10
EXPIRATION AND TERMINATION

10.1 CDIC may terminate this Agreement at any time by giving the Supplier ten (10) business days prior written notice. The Supplier and CDIC agree and acknowledge that the giving of such written notice shall serve to discharge all liability whether contractual, statutory, or otherwise owed by CDIC to the Supplier, except CDIC's obligation to pay the Supplier any outstanding Fees earned and GST/HST/PST thereon, and any Disbursements or Pre-approved Expenses incurred by the Supplier in the period prior to the effective date of termination of this Agreement which obligation shall survive such termination.

10.2 If the Supplier breaches any provision of this Agreement and fails to remedy such breach within five (5) Business Days of receiving a written notice from CDIC notifying the

Supplier of such breach, CDIC may, without giving any further notice to the Supplier, terminate this Agreement effective as of the end of such five (5) day period.

10.3 Notwithstanding any other provision of this Agreement, if this Agreement is terminated by CDIC pursuant to Section 10.2 above:

(a) the Supplier shall not be entitled to payment for any amount on account of Fees, GST/HST/PST, Disbursements or Pre-approved Expenses that are charged or incurred by the Supplier after the day upon which such notice of breach of the Agreement is received by the Supplier; and,

(b) CDIC may arrange, upon such terms and conditions and in such manner as CDIC deems appropriate, for any uncompleted Services to be completed and the Supplier shall be liable to CDIC for any amounts in excess of the Total Fee as are required to retain a replacement Supplier to complete the Services as per each Task Authorization. CDIC may, in its sole discretion, withhold from the amount due to the Supplier upon termination of this Agreement such sums as CDIC determines to be necessary to protect CDIC against any excess costs it might incur in relation to the retention of a replacement Supplier and the completion of the Services.

10.4 If the Services are not provided in full, the Supplier shall be entitled to payment of that portion of the Total Fee per Task Authorization represented by the Services performed as determined by CDIC acting reasonably and based on the agreed upon scope of Services.

10.5 A particular Task Authorization shall expire automatically on the earlier of the required completion date or the date on which the Services are completed by the Supplier for a particular Task Authorization and Accepted by the Designated Officer.

10.6 Upon expiration or termination of this Agreement for any reason whatsoever, the Supplier shall forthwith return all Information, Confidential Information, Work Product and other materials embodying CDIC's Intellectual Property Rights in the possession or control of the Supplier or any Assigned Person to CDIC or shall provide a written certificate to CDIC certifying the destruction of all Information, Confidential Information, Work Product and other materials embodying CDIC's Intellectual Property Rights if instructed by CDIC to destroy such Information.

ARTICLE 11
INDEMNIFICATION

11.1 CDIC agrees to indemnify, defend and hold harmless the Supplier and its respective employees, agents, officers, directors, successors and assigns (each, a "**Supplier Indemnitee**"), from and against any Claims that may be made or brought against the Supplier Indemnitee, or which they may suffer or incur, directly as a result of any deliberate or negligent acts or omissions by CDIC or any person for whom CDIC is responsible.

11.2 The Supplier agrees to indemnify, defend and hold harmless CDIC and its respective employees, agents, officers, directors, successors and assigns (each, a "**CDIC Indemnitee**") from and against any Claims that may be made or brought against the CDIC

Indemnitee, or which they may suffer or incur, directly or indirectly as a result of or in connection with:

(a) any deliberate or negligent acts or omissions of the Supplier or any person for whom the Supplier is responsible (including any Assigned Person);

(b) any injury sustained by the Supplier or by any Assigned Person while on the Premises for any reason connected with this Agreement;

(c) the infringement, alleged infringement or potential infringement by any aspect of the Services or the Work Product of the Intellectual Property Rights of any person;

(d) any breach by the Supplier or any Assigned Person of Article 4 or the obligations to protect Confidential Information or Personal Information; or

(e) any other breach of this Agreement by the Supplier or by any Assigned Person.

11.3 The obligation to indemnify in respect of any Claim is contingent upon the CDIC Indemnitee or the Supplier Indemnitee (as applicable) (the "**Indemnified Party**") (a) giving prompt written notice thereof to the indemnifying Party (the "**Indemnifying Party**") and (b) providing reasonable co-operation and assistance to the Indemnifying Party in the investigation, defence, negotiation and settlement of any Claim, including providing reasonable access to relevant information and employees. The obligation to indemnify in respect of any Claim shall terminate unless the Indemnified Party gives the aforementioned written notice to the Indemnifying Party within two (2) years of the date on which the Indemnified Party knew or ought reasonably to have known of the existence of the Claim.

11.4 **Third Party Claims**. In respect of any third party Claim, the Indemnifying Party will be entitled to elect by written notice addressed to the Indemnified Party, within fifteen (15) days after its receipt of such notice, to assume control over the investigation, defence, negotiation and settlement of such third party Claim at its own cost, risk and expense.

(a) If the Indemnifying Party elects to assume such control, the Indemnified Party will have the right to participate in the investigation, defence, negotiation and settlement of such third party claim at the cost of the Indemnifying Party and to retain counsel to act on its behalf, provided that the fees and disbursements of such counsel will be paid by the Indemnified Party unless the Indemnifying Party consents to the retention of such counsel or unless the named parties to any action or proceeding include both the Indemnifying Party and the Indemnified Party and the representation of both the Indemnifying Party and the Indemnified Party by the same counsel would be inappropriate due to the actual or reasonably potential differing interests between them (such as the availability of different defences). The Indemnifying Party will not settle any Claim without the prior written consent of the Indemnified Party.

(b) If the Indemnifying Party does not elect to assume control of the investigation, defence, negotiation and settlement of the third party Claim, or if the Indemnifying

Party, having elected to assume such control thereafter fails to diligently defend the third party Claim, the Indemnified Party will have the right to assume such control in such reasonable manner as it may deem appropriate, at the cost, risk and expense of the Indemnifying Party, and the Indemnifying Party will be bound by the results obtained by the Indemnified Party with respect to such third party Claim. The Indemnifying Party will have the right to participate in such defence at its own cost and expense.

11.5 **Set-off and Subrogation**. The indemnity obligations hereunder will be enforceable without right of set-off, counterclaim or defence as against the Indemnified Party. The Indemnifying Party will, upon payment of an indemnity in full under this Agreement, be subrogated to all rights of the Indemnified Party with respect to the claims and defences to which such indemnification relates.

ARTICLE 12
DISPUTE RESOLUTION

12.1 Subject to Section 12.4 below, all matters to be decided or agreed upon by the Parties under this Agreement and all disputes which may arise with respect to any matter governed by this Agreement shall at first instance be decided or resolved by the most senior Assigned Person or Designated Officer of each Party. Each Party acknowledges that it is in their mutual best interests to make all such decisions by mutual agreement and agrees to act reasonably and in good faith in order to permit and encourage their employees and officers to do so.

12.2 If the Assigned Person or Designated Officer noted above are not able to resolve any dispute referred to them within fifteen (15) days of such referral, or if they are not able to agree on any other matter required to be decided by them under this Agreement, either Party may refer the matter to arbitration in accordance with the provisions of the *Commercial Arbitration Act*, R.S.C., 1985, c. 17 (2nd Supp.).

12.3 No Party may bring legal proceedings in respect of any issue that is to be submitted to arbitration hereunder unless that Party has complied with subsection 12.1 and 12.2.

12.4 Notwithstanding the above, each Party reserves the right to seek equitable relief in a court of competent jurisdiction to protect Intellectual Property Rights, Confidential Information or Personal Information.

ARTICLE 13
FORCE MAJEURE

13.1 Neither Party shall be liable for any default or delay in the performance of its obligations under this Agreement: (i) if and to the extent such default or delay is caused by: fire, flood, hurricane, earthquake, elements of nature or acts of God, pandemic, epidemic, war, terrorism, explosion, riots, civil disorders, rebellions or revolutions in any country; or any other unforeseeable cause beyond the reasonable control of such Party, and (ii) provided

the non performing Party is without fault in causing such default or delay, and such default or delay could not have been prevented by reasonable precautions (including the disaster recovery plan of the non-performing Party) and cannot be circumvented by the non performing Party through the use of alternate sources, workaround plans or other means (any such event is referred to as a "**Force Majeure Event**").

13.2 Any Party so delayed in its performance shall promptly notify the Party to whom performance is due, by email and describe at a reasonable level of detail the circumstances causing such delay.

13.3 Neither Party shall, by reason of a Force Majeure Event, be entitled to terminate this Agreement nor shall either Party have any claim against the other in respect of such non-performance or delay in performance, unless the performance in whole or part of any obligation under this Agreement is delayed by reason of any such Force Majeure Event for a period exceeding three (3) months after which, either Party shall have the right to terminate the Agreement. In the event that a Party terminates the Agreement because of an Force Majeure Event, neither Party shall have any liability to the other Party, financial or otherwise.

13.4 For the purposes of this provision, the Covid-19 pandemic shall not constitute an event of Force Majeure.

ARTICLE 14
INSURANCE

14.1 The Supplier shall obtain and maintain in force throughout the term of this Agreement and for a minimum period of one (1) year after expiration or termination of this Agreement:

(a) Commercial general liability insurance in an amount not less than five million ($5,000,000.00) inclusive per occurrence. The policy shall add Canada Deposit Insurance Corporation (CDIC) as an additional insured. The coverage provided shall include, at a minimum, the following:

(i) Premises and operations;

(ii) Broad form products and completed operations;

(iii) Bodily injury, including death;

(iv) Broad form property damage;

(v) Personal injury;

(vi) Broad form blanket contractual;

(vii) Waiver of subrogation in favour of CDIC;

(viii) Non-owned automobile, including contractual;

(ix) Contingent employers' liability;

(x) Employees, consultants and sub-contractors as insureds;

(xi) Cross liability; and

(xii) Severability of interest.

(b) Crime insurance in an amount of not less than five million ($5,000,000.00) per occurrence, such insurance to extend to losses CDIC might suffer as a result of fraudulent or dishonest acts of the Supplier's employees, agents, subcontractors or Assigned Persons in performing any or all of the Services under this Agreement.

(c) Technology Professional Liability insurance for financial loss arising out of an error, omission or negligent act in the rendering of Services in an amount not less than ten million ($10,000,000.00) per claim and twenty million ($20,000,000.00) aggregate. Such policy shall be on a claims-made basis and shall provide coverage for damages and defense costs. The Technology Professional Liability policy will also include an insuring agreement for cyber or network security and privacy liability insurance, covering financial loss arising out of actual or potential unauthorized access, unauthorized use, and a failure to protect confidential information which results in loss or misappropriation of such information in both electronic and non-electronic format. Such insurance will have a limit of an amount not less than ten million ($10,000,000.00) per claim and twenty million ($20,000,000.00) aggregate. Notwithstanding this Section 14.1, the Supplier shall maintain said liability coverage in place for a three (3)-year time period after termination of the Agreement by way of annual policy renewal, or purchase of extended reporting period.

All the above insurance policies shall contain an endorsement by the Supplier's insurer to provide the CDIC with thirty (30) days prior written notice of cancellation or material change in risk.

14.2 Evidence of Insurance

The Supplier shall deliver to CDIC, prior to the commencement of the Services under this Agreement, certificates of insurance evidencing coverage in Section 14.1. During the term of the Agreement, the Supplier shall provide evidence that all such policies are in full force and effect by way of certificates of insurance:

(a) Annually; or

(b) If there are mid-term amendments to coverage which could adversely impact CDIC, at the time the change is effected; or

(c) At any time, at CDIC's request.

14.3 Compliance with this Article 14 will not relieve the Supplier from compliance with any other obligation set out in this Agreement and will not limit the insurance coverage that the Supplier is required to carry under municipal, provincial or federal law.

14.4 Without limiting the generality of the foregoing, the Supplier will determine what additional insurance coverage is necessary for its own protection and to fulfill its obligations under this Agreement. The Supplier will provide and maintain any such additional insurance.

ARTICLE 15
SURVIVAL OF TERMS OF AGREEMENT

15.1 All of:

(a) the Supplier's and any Assigned Person's obligations regarding confidentiality of information and ownership of Intellectual Property Rights under Articles 4 and 7 and Appendix C;

(b) the provisions regarding indemnification; and

(c) the provisions regarding dispute resolution,

shall survive the expiration or termination of this Agreement for any reason whatsoever, as shall any other provision of this Agreement which, by the nature of the rights or obligations set out therein, might reasonably be expected to so survive.

ARTICLE 16
GENERAL

16.1 **Entire Agreement**. This Agreement constitutes the entire agreement between the Parties pertaining to the subject matter of this Agreement and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, of the Parties pertaining to that subject matter. No supplement, modification or waiver or termination of this Agreement shall be binding unless executed in writing by the Party to be bound thereby.

16.2 **Amendments**. This Agreement may be changed, amended or modified at any time by written instrument executed by the authorized representatives of the Parties, except for amendments to the Assigned Persons listed in a particular Task Authorization pursuant to Section 6.5 which only require the written consent of CDIC.

16.3 **Intentionally Omitted.**

16.4 **Waiver**. No term or provision of this Agreement shall be deemed waived and no breach thereof shall be deemed excused unless such waiver or consent is in writing and signed by the Party waiving or consenting. No waiver or consent by any Party, whether express or implied, shall constitute a waiver or consent for any other term or provision or subsequent breach of such term or provision.

16.5 **Assignment**. Neither this Agreement nor any part of, nor any right, title or interest under this Agreement shall be assigned, sub-contracted or otherwise transferred by the Supplier without CDIC's prior written consent, which consent may be withheld without reason. This Agreement shall enure to the benefit of and bind the Supplier and its successors and permitted assigns.

16.6 **Publicity**. The Supplier shall not refer to this Agreement, nor to any of its rights or obligations under this Agreement, in any public forum, or for the purpose of promoting itself or its products or services, without the prior written consent of CDIC. The Supplier acknowledges that CDIC is subject to the *Access to Information Act* and, as a consequence, CDIC may be required to disclose any information contained in this Agreement including, but not limited to, the name of the Supplier and/or any Assigned Person, the Total Fee, the description of the Services and any Work Product arising therefrom. The Supplier also acknowledges that CDIC may refer to any information contained in this Agreement on its website.

16.7 **No Solicitation**. The Parties agree that, unless otherwise agreed to by the Parties in writing, during the term of this Agreement neither Party shall directly or indirectly solicit as an employee or independent contractor an employee of or consultant to the other Party or a former employee of or consultant to the other Party that is or was involved in providing the Services under this Agreement.

16.8 **Relationship between the Parties**. During the term of this Agreement and for all purposes whatsoever relating thereto, Supplier is and will be an independent contractor engaged under contract for the provision of Services for CDIC. Supplier will not be a servant or employee of CDIC. This Agreement is not a partnership between or joint venture by the Parties hereto and neither Party is the agent of the other Party. This Agreement is not for the benefit of any third party, whether or not referred to herein.

16.9 **Severability**. If any of the provisions contained in this Agreement are found by a court of competent jurisdiction to be invalid, illegal or unenforceable in any respect, the validity, legality or enforceability of the remaining provisions contained herein shall not in any way be affected or impaired thereby.

16.10 **Further Assurances**. The Parties hereto agree, from time to time after the execution of this Agreement, to make, do, execute or cause or permit to be made, done or executed all such further and other lawful acts, deeds, things, devices, conveyances and assurances in law whatsoever as may be required to carry out the true intention and to give full force and effect to this Agreement.

16.11 **Enforceability**. Each Party affirms that it has full power and authority to enter into and perform the terms of this Agreement, and that the person(s) signing this Agreement on behalf of each Party is (are) properly authorized and empowered to sign it. Each Party further acknowledges that prior to execution of this Agreement, it has read this Agreement, has had the opportunity to be advised by an independent legal advisor if it so desired, and that it understands and agrees to be bound by this Agreement.

16.12 **Conflict**. In the event of any conflict or inconsistency between this Agreement and the appendices to this Agreement, the terms and conditions set out in this Agreement shall prevail.

16.13 **Remedies**. The remedies expressly stated in this Agreement shall be cumulative and in addition to and not in substitution for those generally available at law or in equity.

16.14 **Notices**. Any notice required or permitted to be given hereunder in writing may be delivered (including by commercial courier) or sent by facsimile, email or other electronic transmission. Delivered notices shall be deemed received upon delivery during business hours. Notices sent by facsimile, email or other electronic transmission or delivered outside of business hours shall be deemed received on the next Business Day following the day of transmission or delivery. The addresses to be used for any deliveries or transmissions may be changed by notice given in accordance with this Section and, until so changed, shall be as follows:

if to the Supplier:

<*name + address*>

Attention: <*name*>, <*title*>

Fax: <*>
Telephone: <*>
Email: <*>

and if to CDIC:

Canada Deposit Insurance Corporation
50 O'Connor Street, 17th Floor
Ottawa, ON K1P 6L2

Attention: <*name*>, <*title*>

Telephone: (613) <*>
Email: <*>@cdic.ca

16.15 **Survival**. The provisions of this Agreement which contemplate performance or obligations beyond its termination, including those relating to warranties, indemnification, liability, intellectual property, confidentiality, privacy, audit rights, dispute resolution and choice of law provisions, shall survive any termination or expiry of this Agreement.

16.16 Counterparts. This Agreement may be executed in any number of counterparts. Either Party may send a copy of its executed counterpart to the other Party by facsimile, email or other electronic transmission instead of delivering a signed original of that counterpart. Each executed counterpart (including each copy sent by other means) will be deemed to be an original; all executed counterparts taken together will constitute one agreement.

THE PARTIES HAVE EXECUTED this Agreement as of the latest date this Agreement is signed by all the Parties (the "**Execution Date**").

CANADA DEPOSIT INSURANCE CORPORATION

Name: <*>
Title: <*>

Date:

I have authority to bind the above corporation.

[Supplier's Name in Caps]

Name: **[Supplier's Representative's Name]**

Title: <*>

Date:

I have authority to bind the above corporation.

Appendix A
SERVICES AND FEES

1. Description of Services

The Supplier agrees to provide to CDIC certain services (the "**Services**") in respect of the Service Stream(s), Service Categories and/or Roles for which the Supplier has qualified, as outlined in Appendix B and the Supplier's Proposal (the "**Proposal**") dated <*> submitted in response to the RFSA.

In the event of any conflict or inconsistency between the documentation, the order of precedence shall be as follows: (i) this Appendix A; (ii) the Agreement; and (ii) the Supplier's Proposal.

2. Service Request Process

CDIC may issue a written Service Request to the Supplier and to other suppliers selected pursuant to this RFSA, setting out a brief description of the Services and deliverables required, the timeframes, and any other requirements.

If the Supplier wishes to respond to a Service Request, the Supplier shall prepare, at no cost to CDIC, a written response delivered to CDIC setting out: the list and description of the deliverables; the names and resumes of the resources that the Supplier proposes to assign to each of the Roles (if applicable); the estimated duration for each resource required to achieve completion of the proposed Services within the timeframe specified in the Service Request; the proposed fees (including a detailed breakdown of the fees for particular Services and/or deliverables); and the applicable milestones. The Supplier's response to the Service Request shall comply with the requirements set out in the Service Request. The Supplier shall ensure that each individual proposed is qualified for the Role. The Supplier shall provide CDIC or its representatives with the opportunity to interview its proposed resource(s), at no cost.

If the Supplier receives a Service Request but does not intend to submit a response, the Supplier shall notify CDIC that it will not respond.

3. Task Authorization

Upon CDIC's acceptance of a Supplier's satisfactory response to the requirements set out in the Service Request, both parties must provide approval in writing, resulting in a Task Authorization, which authorizes Services to commence.

CDIC will issue an amendment to the Task Authorization in the event of any changes to the scope of the Services, activities to be performed, or changes in any schedules that may be necessary or desirable in light of additional information or actual experience obtained prior to, or in the course of the Services, or as CDIC redefines its needs.

CDIC will not pay the Supplier for any design changes, modifications or interpretations of the Services unless they have been approved, in writing, and CDIC has issued a Task Authorization amendment authorizing the increased expenditure to be incorporated into the work.

CDIC may terminate all or any part of an authorized Task Authorization for the convenience of CDIC on ten (10) days written notice to the Supplier. In the event of such termination, the Supplier agrees that it will be entitled to be compensated only for work performed and accepted up to the effective date of such termination.

CDIC may terminate all or any part of an authorized Task Authorization due to the default of the Supplier at any time on ten (10) day's written notice to the Supplier provided the Supplier has not rectified the default during the notice period. In the event of such termination, the Supplier and CDIC agree that the rights and obligations of the Supplier and CDIC will be governed by the provisions of Article 10 (Expiration and Termination).

4. Term

Subject to any earlier termination by CDIC pursuant to the Agreement, the term of this Agreement shall be:

Commencement Date: Execution Date
Completion Date: December 31, 2026

5. Fees

The Supplier agrees to provide the Services at the rates (the "**Fees**") set out in Appendix B for the duration of the term.

6. Payment Scheduling

The Supplier shall provide an Invoice to CDIC upon completion and Acceptance of the Services.

7. CDIC Designated Officer

Name: <*>
Title: <*>

8. Disclosure Regarding Non-Compliant Jurisdictions

[Insert "None" or describe any disclosures re: Article 4 of the Agreement, if any]

9. Subcontractor(s): [*Insert if applicable*]

If required, CDIC acknowledges that some of the Services will be subcontracted by the Supplier to [insert name of subcontractor(s)], pursuant to an arrangement between the Supplier and the subcontractor. CDIC hereby consents to such portion of the Services, as reasonably determined by the Supplier, being completed by the foregoing subcontractor(s).

Appendix B
SERVICE STREAM(S), SERVICE CATEGORIES/ROLES

For a description of "Service Categories" and "Roles", refer to RFSA.

Service Stream # <*>: <*>

1. **Qualified Service Stream(s), Service Categories and Roles**

   Supplier is qualified to provide services in the following Service Categories and Roles indicated below in this Appendix for Service Stream #<*>.

   [Instructions: Insert chart for particular Service Stream.]

2. **Fees**

   All fees for Service Stream #<*> will be calculated based on hourly rates. The Parties confirm that the Total Fee to be paid by CDIC to the Supplier for the completion of the Services shall not exceed the Total Fees as set out in a particular Task Authorization related to the Services being performed.

   The Supplier agrees to provide the Services at the following all-inclusive hourly ceiling rates (the "**Fees**"):

   [Insert tables]

   The above hourly rates are applicable for the full Term of the Agreement.

   The Supplier shall ensure that Services provided will be assigned to the Assigned Person(s) at the lowest hourly rate(s) who is (are) competent to provide the Services.

AND/OR

.

[Service Stream #<*>: Project Delivery Services]

1. **Qualified Service Stream(s), Service Categories**

Supplier is qualified to provide services in the following Service Categories for Service Stream # <*>:

Service Category #<*>

2. Fees

For Service Stream #<*>, the Parties confirm that the Total Fee to be paid by CDIC to the Supplier for the completion of the Services shall not exceed the Total Fees as set out in a particular Task Authorization for Services outlined therein.

[Insert tables]

Appendix C
CONFIDENTIALITY, PRIVACY, CONFLICT OF INTEREST AND SECURITY

Any capitalized terms used herein but not defined have the meaning set out in the Agreement.

Confidentiality:

1. "**Confidential Information**" means

   (a) any and all technical and non-technical information including patents, copyrights, trade secrets, proprietary information, techniques, sketches, drawings, models, inventions, know-how, processes, apparatus, equipment, algorithms, software programs, software source documents, and formulae related to existing, proposed and future products and services;

   (b) information concerning research, experiments, procurement requirements, manufacturing, customer lists, business forecasts, sales, merchandising and marketing plans;

   (c) proprietary or confidential information of any third party that may rightfully be disclosed by CDIC to the Supplier;

   (d) information which is expressly communicated as being or is marked as confidential;

   (e) information which by its nature and the context in which it is disclosed is confidential;

   (f) all information regarding CDIC or any of its business affairs, liabilities, assets, plans or prospects, including any and all information in respect to the Services and the provision of those Services;

   (g) all information regarding any member or former member institution of CDIC, any parent or subsidiary corporation or affiliate thereof, or any of the business affairs, liabilities, assets, plans or prospects of any member or former member institution of CDIC or any parent or subsidiary corporation or affiliate thereof, disclosed to or received by the Supplier during or as a result of providing the Services, whether originating from CDIC or any other source; and

   (h) all Work Product.

2. The Supplier shall not disclose any Confidential Information, unless such disclosure:

   a. is compelled:

      i. by law in connection with proceedings before a court, commission of inquiry or other public tribunal of competent jurisdiction;

      ii. by law at the request of any regulatory or supervisory authority having jurisdiction; or

      iii. in accordance with the practices and procedures of Parliament (including any committee of the House of Commons or Senate of Canada);

b. is of information that is in the public domain or has come into the public domain other than by reason of a breach of this Appendix (and, for the purpose hereof, information is not considered to be in the public domain merely because it appears in a court file or other repository to which members of the public are capable of having access, but only if it has actually been disseminated to the general public, such as through the news media or the publication of annual or other reports);

c. is of information that has been, or is hereafter, received by the Supplier or any Assigned Person other than from or at the request of CDIC and other than during or as a result of providing the Services;

d. is part of the performance of any part of the Services which is to be done on a shared, cooperative or joint basis with such other persons at the request, or with the concurrence of the Designated Officer who have signed an agreement similar in form and substance to this Appendix; or

e. is made with the prior written consent of the Designated Officer.

3. If the Supplier believes that disclosure of Confidential Information is or is about to be required in one of the circumstances described in subsection 2.a, or in any circumstances not referred to in Section 2, it shall notify CDIC orally as soon as reasonably possible and as much in advance of the impending disclosure as possible, of the circumstances and scope of the disclosure and shall immediately confirm such oral notice in writing.

4. The Supplier agrees that it acquires no right, title or interest to any Confidential Information, except a limited right to use the Confidential Information in connection with the provision of the Services. All Confidential Information remains the property of CDIC or its members and no licence or other right, title or interest in the Confidential Information is granted hereby.

5. The Supplier agrees to protect the Confidential Information and prevent any wrongful use, dissemination or publication of the Confidential Information not permitted hereunder by a reasonable degree of care, but no less than the degree of care used to protect its own confidential information of a like nature.

6. On receipt of a written demand from CDIC, the Supplier shall immediately return all Confidential Information, including any copies thereof, and any memoranda, notes or other documents relating to the Confidential Information (the "**Confidential Material**"), or shall provide a written certificate to CDIC certifying the destruction of all Confidential Information and Confidential Material and other materials embodying CDIC Intellectual Property if instructed by CDIC to destroy such Information.

7. The Supplier acknowledges and accepts that, in the event of any breach or anticipated breach of this Appendix, damages alone would not be an adequate remedy, and agree that CDIC shall be entitled to seek equitable relief, such as an injunction, in addition to or in lieu of damages and without being required to prove that it has suffered or is likely to suffer damages.

8. All Confidential Information is provided "AS IS" and without any warranty, express, implied or otherwise, regarding its accuracy.

9. Unless expressly authorized in this Agreement or by CDIC in writing, Supplier shall, in accordance with reasonable industry standards, enforce policies, procedures and access control mechanisms to prevent the merger, linking or commingling of any Confidential Information or Personal Information with its own data or the data of any other person.

Privacy:

10. If CDIC intends to provide the Supplier with (or allow the Supplier to access or collect on CDIC's behalf) any Personal Information as part of the Services, CDIC shall advise the Supplier of this fact, and the Supplier shall be required to comply with the following privacy obligations.

11. The Supplier shall comply at all times with all applicable Canadian laws and regulations relating to the collection, creation, use, storage and disclosure of Personal Information, and for greater certainty shall conduct itself so as to ensure that the Services comply with the Canadian *Privacy Act*.

12. The Supplier shall provide a copy of, or, where appropriate, a reference to, a privacy notice in a form acceptable to CDIC when collecting Personal Information on behalf of CDIC.

13. The Supplier shall not use or disclose any Personal Information except to the extent required to perform obligations under the Agreement or as otherwise permitted under applicable law. If, in performing its obligations under the Agreement, the Supplier is required to disclose Personal Information to a third party, the Supplier shall, prior to disclosing such Personal Information, advise CDIC in writing of the proposed use of the Personal Information by the third party. If CDIC consents to the disclosure, the Supplier shall require the third party to enter into an agreement imposing obligations upon the third party with respect to the collection, use and disclosure of the Personal Information that are substantially similar to the obligations set out herein, failing which, the Personal Information shall not be disclosed except in accordance with applicable law.

14. The Supplier shall promptly notify CDIC in writing and assist CDIC in resolving any claim, inquiry, active or pending investigation, complaint that is made to the Supplier or filed with competent authorities, or any remedial action that either has been ordered to take by competent authorities regarding the collection, storage, use or disclosure of Personal Information by the Supplier.

15. The Supplier shall retain the Personal Information only for so long as is reasonably necessary to complete the purposes for which the Personal Information was provided and as otherwise permitted by applicable law, unless otherwise specified by CDIC in writing (collectively, the "**Retention Period**") – and upon the expiry of the Retention Period, shall return to CDIC, or as directed by CDIC, delete or destroy the Personal Information. The Retention Period shall (unless otherwise specified by CDIC in writing) automatically expire on the date on which the Agreement expires or is terminated for any reason whatsoever. Upon request, the Supplier shall provide CDIC with a written certificate certifying the destruction of the Personal Information or the return to CDIC of all Personal Information (as applicable).

Conflict of interest:

16. CDIC requires any persons entering into any agreement with CDIC, supplying services to, or performing any work for or in regards to CDIC, to conduct their affairs in such a way as to avoid any conflict of interest. The Supplier hereby represents and declares that, after due inquiry, it is not aware of any circumstances which do or might cause the Supplier to have a conflict of interest in carrying out the Services. The Supplier agrees not to enter into any contract or other commitment with any person during the term of the Agreement that would cause a conflict of interest on the Supplier's part in connection with the performance of the Services.

Security:

Protection of Information

17. The Supplier confirms that Services involving Personal Information or other "**Protected Information**", as that term is defined in CDIC's *Information Classification Standard* will be handled in accordance with CDIC's *IT Asset and Information Handling Standard* and *Cryptography Procedure* and other security procedures, as applicable. Where the Supplier cannot meet the requirements of the procedure, Services involving Personal Information or other Protected Information will be performed on CDIC's premises only, using CDIC computer systems exclusively or, where applicable, specific remote access or other technology approved by CDIC in writing ("**Access Technology**" as set out below). The Supplier shall require that no Protected Information is removed from CDIC premises at any time during the Term of the Agreement, except where transmitted using the Access Technology.

    CDIC has adopted Access Technology as a means for the secure electronic transmission of designated information, classified up to a Protected "B" level, over the Internet. In order for CDIC to provide Access Technology accounts to any Assigned Persons, the Supplier agrees that the Supplier shall, in addition to any other term herein, use the Access Technology in accordance with the following terms and conditions:

    (i) CDIC shall designate one or more Assigned Persons to be known as Token Registration Authorities ("**TRAs**") who shall be responsible for coordinating the applications by, and for verifying the identify of, each Assigned Person for whom CDIC agrees to provide an Access Technology account;

    (ii) CDIC reserves the right to refuse to issue an Access Technology account to any or all Assigned Persons;

    (iii) Supplier shall be required to complete application forms to obtain Access Technology tokens with the approval of CDIC, together with training to be provided by CDIC concerning the administration of the Access Technology;

    (iv) The Supplier shall require all Assigned Persons with Access Technology accounts to keep their respective Access Technology tokens and passwords confidential, and to take all reasonable measures to prevent the loss, unauthorized disclosure, modification or improper use of any Access

Technology token or associated password.

The Supplier shall prohibit each Assigned Person from sharing their Access Technology token or associated password with any other person;

(v) The Supplier shall require that all CDIC data accessed and modified by the Supplier and its Assigned Persons while using the Access Technology is re-saved only to the CDIC network. The Supplier and its Assigned Persons shall not transfer, save or send any copies of CDIC data to a non- CDIC computer system, nor create hard copies of the data, without the express written consent of CDIC;

(vi) The Supplier shall promptly advise CDIC if any Assigned Person's Access Technology token or associated password is, was or may be compromised or not secure, and shall likewise require Assigned Persons to promptly report any such incidents to the Supplier;

(vii) The Supplier shall promptly advise CDIC if (a) any Assigned Person ceases to be involved in providing the Services or (b) any of the information contained in an Assigned Person's Access Technology application changes or becomes otherwise inaccurate or incomplete;

(viii) The Supplier acknowledges and agrees that the Access Technology is for the sole use of the Supplier in connection with the delivery of the Services to CDIC. The Supplier shall not permit anyone other than an approved Assigned Person and CDIC to access the Access Technology and related software, or to authenticate Access Technology passwords in accordance with this Agreement;

(ix) The Supplier shall require that any operating software and computer virus software that is installed on all computer systems to be used by the Assigned Persons in connection with the Access Technology is acceptable to CDIC, and will update or install such software as CDIC may request to maintain the security of the Protected Information. The Supplier acknowledges that if the software required by CDIC is not installed properly on any computer systems used by Assigned Persons in connection with the Services, then access to the Access Technology and the CDIC network, and any use of the Access Technology , may be denied and will be at the Supplier's risk;

(x) CDIC reserves the right to revoke or modify any Access Technology account provided to any Assigned Person at any time, without notice and in its sole discretion, including without limitation if a Access Technology token or password was, is or is suspected of being compromised, or if an Assigned Person is no longer involved in providing the Services. All Access Technology accounts shall be revoked by CDIC and all Access Technology tokens promptly returned by the Supplier when the Agreement between CDIC and the Supplier expires or is terminated, whichever occurs earlier;

(xi) The Supplier acknowledges that the Access Technology software is subject to intellectual property licenses and restrictions and agrees to adhere to the terms and conditions outlined in this Agreement concerning the use of such

software. In particular, and without limiting the generality of other provisions in this Agreement, the Supplier shall not tamper with, alter, destroy, modify, reverse engineer, decompile, or abuse the Access Technology software or tokens in any way, nor distribute or use the software or tokens for any purpose other than for dealings with CDIC;

(xii) The Supplier acknowledges and agrees that it shall be jointly and severally liable with each Assigned Person for any breach of the above terms concerning the use of the Access Technology software by any such Assigned Person; and

(xiii) CDIC cannot warrant or represent that the Access Technology will be always available or functional, including without limitation because of events such as system maintenance and repair, or events outside the reasonable control of CDIC, or that occurred without the fault or neglect of CDIC.

Security Clearance

18. If the performance of the Services involves Personal Information or other Protected Information, the Supplier shall require that all the Assigned Persons or any Subcontractors' personnel who will perform the Services either:

    (a) as of the Commencement Date, have a minimum security clearance of "Reliability", as that term is defined in CDIC's *Personnel Security Standard* or such other security clearance level as requested by CDIC; or

    (b) within one (1) week of the Commencement Date, the Supplier will apply to obtain the necessary security clearance.

    The Supplier agrees that once the required level of security clearance is obtained by an Assigned Person or any Subcontractor's personnel, it shall cause each Assigned Person or Subcontractor's personnel to maintain his or her respective security clearance for the duration of his or her work during the term of the Agreement.

Appendix D
SERVICE REQUEST AND TASK AUTHORIZATION FORM

(SAMPLE ONLY)

All correspondence and invoices **MUST** show the Service Request Number and Professional Services Agreement number.

<table>
<tr><th colspan="2">SECTION 1: Service Request Details</th></tr>
<tr><td>Service Request Number:</td><td>Professional Services Agreement Number:</td></tr>
<tr><td>Service Request Type: <Select one of the following>

☐ Direct
☐ Mini-Quotation (issued to multiple Suppliers)</td><td>Service Request Title:</td></tr>
<tr><td rowspan="2">To: <Supplier Name and Address></td><td>Date of Service Request Issuance:</td></tr>
<tr><td>Response Required by:</td></tr>
<tr><td rowspan="2">Service Stream:</td><td>Required Commencement Date:</td></tr>
<tr><td>Required Completion Date:</td></tr>
<tr><td>Option Period:</td><td></td></tr>
<tr><td colspan="2">Trade Agreements: <insert if applicable></td></tr>
<tr><td colspan="2">Required Resource <Role/Function> and Levels:

CDIC requires the Services of the following:

<table>
<tr><th>Service Category</th><th><Role/Function></th><th>Level</th><th>Estimated No. of Hours
(1 Day = 7 Hours)</th></tr>
<tr><td><Insert Service Category Number and Title></td><td><Insert Role/Function Title and Number></td><td><Insert Role/Function Level></td><td>** Days @ 7 Hours/Day = ** Hours</td></tr>
</table>
</td></tr>
<tr><td colspan="2">Description of Duties and Responsibilities: <Insert description of the specific duties and responsibilities required as described in the RFSA></td></tr>
<tr><td colspan="2">Additional Resource Requirements: <Where CDIC requires additional experience, education/certification or qualification requirements as applicable></td></tr>
<tr><td colspan="2">Authorized Location(s) of Work: <Select all that apply>

☐ On-Site (50 O'Connor Street, Ottawa)
☐ On-Site (79 Wellington Street West, Suite 1200, Toronto)
☐ Off-Site / Remote (e.g., Supplier and/or Assigned Person's Premises)</td></tr>
<tr><td colspan="2">Service Request Response Details:</td></tr>
</table>

With its response to this Service Request Form, the Supplier is requested to return the Service Request form i**n its entirety** with Section 2. completed and provide, under a separate cover/attachment <*Insert all that apply*>.

Refined Response Process Details: <*Insert if applicable*>.

Following CDIC's review and assessment of the Supplier's initial Service Request Response, the Supplier may be asked to provide a refined response (e.g., refinement of proposed resources, work plan, effort required and pricing) for CDIC's final evaluation and selection.

Following the issuance of additional refined response submission requirements to Suppliers by CDIC, Suppliers may be eligible to submit a refined response for evaluation and determination by CDIC.

SECTION 2: TO BE COMPLETED BY SUPPLIER (CDICTO SELECT APPLICABLE BASIS OF PAYMENT)

Response Payment Format <*CDIC to select applicable Basis of Payment(s) for the Service Request and delete those that do not apply. Additional rows may be added as required*>

A. Payment on an Hourly Basis (Payment based on Actual Hours of Service Delivered multiplied by Hourly Rate)

Assigned Person (Resource) Name	**Service Category**	**<Role/Function>**	**Level**	**Proposed Hourly Rate**	**No. of Hours**	**Extended Price for Service Request** (Hourly Rate x No. of Hours)
	<*Insert Service Category Number and Title*>	<*Insert Role/Function Title and Number*>	<*Insert Role/Function Level*>	**$**	<*Insert Required Hours the same as above*>	**$**
					Service Request Fee	**$**
					Maximum (GST/PST/HST) Payable (13%)	**$**
					Total Fee for this Service Request	**$**

B. Payment on an Estimated Price Basis (Payment based on Actual Hours of Service Delivery to an overall maximum Total Fee not to exceed the total amount identified below)

Work Product	**Estimated Price per Work Product**	**Estimated number of hours per Work Product**	**Estimated extended price for Statement of Work**
	$		**$**
		Estimated Total Fee	**$**

C. Payment on a Firm/Fixed Price Basis (Payment based on Firm/Fixed Price per Work Product to an overall maximum Total Fee not to exceed the total amount identified below)

Work Product	**Firm/Fixed Price per Work Product** *(hourly rate x no. of hours)*

	$
	$
Firm/Fixed Total Fee	**$**

SECTION 3: TASK AUTHORIZATION – CDIC INTERNAL USE ONLY

Both parties must provide approval in writing below, resulting in a Task Authorization, to authorize Services to commence.

Commencement Date:	**Completion Date:**
We acknowledge receipt of this Service Request # <*Insert Service Request Number*> and agree to deliver the Services in accordance with the Terms and Conditions of the Professional Services Agreement and this Task Authorization. *I have authority to bind the Supplier:* <***Insert Supplier Name***> **Signature:** _____ **Name:** <***Insert Supplier Signatory***> **Title:** <***Insert Supplier Signatory Title***> **Date:** _____	Supplier is authorized to deliver the Services detailed in this Service Request, in accordance with its Service Request Response. *I have authority to bind CDIC:* **CDIC Signature:** _____ **Name:** <***Insert CDIC Signatory***> **Title:** <***Insert CDIC Signatory Title***> **Date:** _____