GREEN ALERT - DUPLEX PRINTING OF THIS DOCUMENT WILL SAVE PAPER

REQUEST FOR PROPOSAL (RFP)

For

Governance Risk & Compliance (GRC) Solution

Request for Proposal (RFP) No.:	RFP 002376
Issued:	February 7, 2024
Submission Deadline**:**	2:00 p.m. EST on March 7, 2024
Address Inquiries to RFP Contact:	Ryan Lemay, Senior Procurement Officer
Email:	rlemay@cmhc-schl.gc.ca

TABLE OF CONTENTS

PART 1 – SUBMISSION INSTRUCTIONS

1.1 OBJECTIVE OF THIS RFP

Canada Mortgage and Housing Corporation ("CMHC") is a Crown Corporation, with a Board of Directors, reporting to Parliament through the Minister of Housing, Infrastructure and Communities. CMHC exists for a single reason: to make housing affordable for everyone in Canada. We know that housing helps people stay employed, do better in school and participate more fully in society. Housing affordability and a stable housing finance system support a stronger, safer Canada where everyone can live with dignity. Affordable housing for all is an ambitious goal, and we cannot do it alone. We're mobilizing the expertise and energy of governments, non-profits, lenders, developers, social entrepreneurs, and co-ops to create the future of housing. Canada's first-ever National Housing Strategy is just one example. Together, we are removing barriers to ensure that no one is left behind. A comprehensive company profile of CMHC can be found at www.cmhc-schl.gc.ca

Vendor Diversity and Inclusion: It is a priority for CMHC to employ a diverse and balanced workforce and suppliers in order to deliver on our aspiration that by 2030 everyone in Canada will have a home that they can afford and meets their needs. This is CMHC's bold aspiration and the basis for our company strategy which outlines the actions that we are taking to address the issues that matter most to Canadians, such as climate change, reconciliation with Indigenous peoples, and anti-racism and equity. It guides our choices, our investment decisions, and the policies and programs we develop and implement. Importantly, our aspiration calls on all of us – governments, housing providers, not-for-profits, the private sector, and others – to seek out innovative ways to achieve housing affordability for all. Working together will be key to creating a truly inclusive society where everyone has the opportunity to thrive.

With this RFP CMHC is seeking prospective proponents to submit proposals for the provision of a cloud-based Software as a Service (SaaS) solution for Governance, Risk and Compliance (GRC) . The requirements include software, licences, on-going support (including training), documentation, maintenance, and implementation services, as further described in Sections A and B of the RFP Specifications (Appendix C).

It is CMHC's intention to enter into an agreement on a non-exclusive basis with the successful proponent. The term of the agreement resulting from this RFP is to be for an initial period of three (3) years, with an option to extend the agreement on the same terms and conditions for up to two (2) additional terms of up to one (1) year. A cumulative total of up to five (5) years.

1.2 RFP CONTACT

For the purposes of this procurement process, the "RFP Contact" will be:

Ryan Lemay, Senior Procurement Officer
rlemay@cmhc-schl.gc.ca

Proponents and their representatives are not permitted to contact any employees, officers, agents, appointed officials or other representatives of CMHC, other than the RFP Contact, concerning matters regarding this RFP. Failure to adhere to this rule may result in the disqualification of the proponent and the rejection of the proponent's proposal.

1.3 TYPE OF CONTRACT FOR DELIVERABLES

The selected proponent will be requested to enter into direct contract negotiations to finalize an agreement with CMHC for the provision of the scope of work and deliverables (collectively the "Deliverables"). The terms and conditions found in the Form of Agreement (Appendix D) are to form the basis for the agreement between CMHC and the selected proponent.

1.4 RFP PROCESS TIMETABLE

RFP Milestone	RFP Dates (2024)
Issue Date of RFP	February 7
Deadline for Questions	February 21
Anticipated response to proponent submitted Questions	March 1
Submission Deadline of proposals	March 7 at 2:00 p.m. EST
Notification of shortlisted proponents	April 10
Presentation from shortlisted proponents	April 22-26
Anticipated Contract Negotiation Period	30 calendar days
Anticipated Execution of Agreement	May

The RFP timetable is tentative only, and may be changed by CMHC at any time. Changes will be communicated in accordance with Section 3.2.2.

1.5 SUBMISSION OF PROPOSALS

1.5.1 PROCUREMENT BUSINESS NUMBER

CMHC utilizes the Supplier Registration Information ("SRI") database maintained by Public Services and Procurement Canada ("PSPC") as the official CMHC source list. All proponents should be registered with PSPC prior to submitting a proposal. The Procurement Business Number ("PBN") provided by this registration must be included with the proponent's proposal. If proponents are not registered and wish to do so, please access https://buyandsell.gc.ca/for-businesses/selling-to-the-government-of-canada/register-as-a-supplier

1.5.2 PROPOSALS TO BE SUBMITTED AT THE PRESCRIBED LOCATION IN PRESCRIBED MANNER

Proposal submissions must be emailed to CMHC's electronic bid submission system ("EBID") to the address indicated below:

Email Address**:** **EBID@cmhc-schl.gc.ca** ("Submission Location")

Proposals sent to any other e-mail address will not be considered.

Please be advised that EBID has a size limitation of 10 MB. Proponents may submit their proposal in multiple smaller files indicating the number of emails submitted (for example: email 1/3, 2/3, 3/3) in the body of the email. Individual files are to be submitted in Microsoft or pdf format.

Note: Rich Text formatted or compressed (zipped) documents cannot be opened by CMHC.

Upon receipt of proposals, an automated confirmation will be issued by EBID to the sender's e-mail address. It is strongly recommended that proponents follow up with the RFP Contact should they not receive said confirmation within thirty (30) minutes of their submission.

1.5.3 PROPOSALS TO BE SUBMITTED ON TIME

Proposals must be submitted pursuant to Section 1.5.2 above and on or before the submission deadline: 2:00 p.m. Eastern Standard Time on March 7, 2024, **Ottawa local time** ("Submission Deadline").

Proposals submitted after the Submission Deadline will be rejected. CMHC does not accept any responsibility for proposals delivered to any other location or by any other means by the proponent. Proponents are advised to make submissions well before the Submission Deadline. Proponents making submissions near this deadline do so at their own risk. Proponents will be deemed to be received when they enter into CMHC's systems and CMHC accepts no responsibility for proposals sent prior to this deadline that fail to enter into CMHC's systems by the Submission Deadline. For the purposes of this section, the time of delivery is deemed to be the time recorded by CMHC's systems.

1.5.4 AMENDMENT OF PROPOSALS

Proponents may amend their proposals prior to the Submission Deadline by submitting the amendment by email prominently marked with the RFP title and number and the full legal name and return address of the proponent to the email address set out above. Any amendment should clearly indicate which part of the proposal the amendment is intended to amend or replace. CMHC will assess the proposal "as is" and CMHC will not correct or accept any responsibility for errors submitted by the proponent.

1.5.5 WITHDRAWAL OF PROPOSALS

At any time throughout the RFP process, a proponent may withdraw a submitted proposal. To withdraw a proposal, a notice of withdrawal must be sent to the RFP Contact and must be signed by an authorized representative of the proponent. CMHC is under no obligation to return withdrawn proposals.

[End of Part 1]

PART 2 – EVALUATION, NEGOTIATION AND AWARD

2.1 STAGES OF EVALUATION AND NEGOTIATION

CMHC will conduct the evaluation of proposals and negotiations in the following stages:

2.1.1 STAGE I – MANDATORY SUBMISSION REQUIREMENTS

Stage I will consist of a review to determine which proposals comply with all of the mandatory submission requirements due at time of submitting the proposal, such as licences or certificates, and detailed in Section H of the RFP Specifications (Appendix C). Should a proponent not include a submission requirement with its proposal, the proponent will be notified by CMHC and will have forty-eight (48) hours from the time of notification to meet this requirement. Only proponents who meet the mandatory submission requirements will move on to the next stage Section 2.1.2 (A).

2.1.2 STAGE II – EVALUATION

Stage II will consist of the following two (2) sub-stages:

MANDATORY TECHNICAL REQUIREMENTS

CMHC will review the proposals to determine whether the mandatory technical requirements of the Deliverables, as detailed in Section I of the RFP Specifications (Appendix C), have been met. The mandatory technical requirements must be met (assessment on a pass/fail basis) before the rated criteria can be considered. Questions or queries on the part of CMHC as to whether a proposal has met the mandatory technical requirements will be subject to the verification and clarification process set out in Section 3.2.4 of Part 3. Only proponents who meet the mandatory technical requirements will move on to the next sub-stage Section 2.1.2 (B).

RATED CRITERIA

CMHC will evaluate each qualified proposal based on the rated criteria as set out in Section K of the RFP Specifications (Appendix C). The evaluation will be conducted by a committee of CMHC employees with the right to vote (the “Evaluation Team”). CMHC may consult with internal subject matter experts without the right to vote (the “Panel”) as applicable during the presentation (Stage IV) of the evaluation process.

2.1.3 STAGE III – PRICING

Stage III will consist of a scoring of the submitted pricing of each qualified proposal in accordance with the price evaluation method set out in the Pricing Form (Appendix B).

2.1.4 STAGE IV – PRESENTATION

Stage IV will consist of a presentation (the "Presentation") by the top three (3) highest scoring proponents to a committee of CMHC employees with the right to vote (the “Evaluation Team”) as set out in Section L of the RFP Specifications (Appendix C) and, if applicable, members of the Panel.

2.2 RANKING AND CONTRACT NEGOTIATIONS

2.2.1 SCORING BY THE EVALUATION TEAM

The following scoring matrix has been developed to assist the Evaluation Team in the scoring process of the rated criteria and the presentation detailed in Appendix C, Section K and Section L:

Score	Evaluation Conclusion	Description
5	Complete and clear description provided that exceeds the requirements of the criteria. No weaknesses or deficiencies that would pose any risk to the proponent's ability to satisfy the requirement.	Outstanding
4	Above average description provided of the proponent's ability to consistently meet key criteria. Minimal weaknesses and/or deficiencies could exist, but would not pose any significant risk to the proponent's ability to satisfy the requirement.	Very Good
3	Average description provided of the proponent's ability to meet key criteria. Minimal weaknesses and/or deficiencies could exist, but would not pose any significant risk to the proponent's ability to satisfy the requirement.	Good
2	Weak information was provided with only a partial description of the proponent's ability to meet the criteria. There are discrepancies and/or deficiencies that pose some risks to the proponent's ability to satisfy the requirement.	Fair
1	Very limited information was provided to assess the proponent's ability to meet the criteria. There are serious discrepancies and/or deficiencies that pose important risks to the proponent's ability to satisfy the requirement.	Unsatisfactory
0	Little or no information provided to assess the proponent's ability to meet the criteria.	No Response

Individual proponent scores will be reviewed and tabulated to reach an average score multiplied by the percentage weighting for each rated criteria except for pricing, which will be evaluated as described in Appendix B – Pricing Form.

2.2.2 RANKING OF PROPONENTS

After the completion of Stage III, all scores from (i) Stage II (B) and (ii) Stage III will be added together, and the proponents will be ranked based on their total scores. The three (3) top ranked proponent(s) will receive a written invitation to Stage IV. After completion of Stage IV, all scores from (i) Stage II (B), (ii) Stage III, and (iii) Stage IV will be added together and the proponents will be ranked based on their total scores. The top-ranked proponent will receive a written invitation to enter into direct contract negotiations to finalize the agreement with CMHC. In the event of a tie, the successful proponent will be the proponent selected by way of negotiations, requiring proponents to answer additional questions, provide supplementary information or make additional presentations such that CMHC may revisit and re-evaluate the proponent's proposal or ranking on the basis of any such information in an effort to select a top-ranked proponent.

2.2.3 CONTRACT NEGOTIATION PROCESS

Any negotiations will be subject to the process rules contained in the Terms and Conditions of the RFP process (Part 3). The negotiation process will not constitute a legally binding offer to enter into a contract on the part of CMHC or the proponent and there will be no legally binding relationship created with any proponent prior to the execution by both CMHC and the proponent of a written agreement. The terms and conditions found in the Form of Agreement (Appendix D) are to form the basis for commencing negotiations between CMHC and the selected proponent. As a part of the negotiation process, CMHC may request supplementary information from the proponent to verify, clarify or supplement the information provided in its proposal or to confirm the conclusions reached in the evaluation and CMHC may include requests for improved pricing or performance terms from the proponent.

2.2.4 TIME PERIOD FOR NEGOTIATIONS

CMHC intends to conclude negotiations and finalize the agreement with the top-ranked proponent during the Contract Negotiation Period, in accordance with the timeframe outlined under Section 1.4 of this RFP. A proponent invited to enter into direct contract negotiations should therefore be prepared to: (i) satisfy the pre-conditions of award listed in Section J of the RFP Specifications (Appendix C), (ii) provide requested information in a timely fashion, and (iii) conduct negotiations expeditiously.

2.2.5 FAILURE TO ENTER INTO AGREEMENT

If the pre-conditions of award listed in Section J of the RFP Specifications (Appendix C) are not satisfied or if the parties cannot conclude negotiations and finalize the agreement for the Deliverables within the contemplated Contract Negotiation Period, pursuant to Section 1.4 of this RFP, then CMHC may discontinue negotiations with the top-ranked proponent and invite the next-best-ranked proponent to enter into negotiations. This process will continue until: (i) an agreement is finalized, (ii) there are no more proponents remaining that are eligible for negotiations or (iii) CMHC elects to cancel the RFP process.

2.2.6 NOTIFICATION OF NEGOTIATION STATUS

Other proponents that may become eligible for contract negotiations may be notified at the commencement of the negotiation process with the top-ranked proponent.

[End of Part 2]

PART 3 – TERMS AND CONDITIONS OF THE RFP PROCESS

3.1 GENERAL INFORMATION AND INSTRUCTIONS

3.1.1 PROPONENTS TO FOLLOW INSTRUCTIONS

Proponents should structure their proposals in accordance with the instructions in this RFP. Where information is requested in this RFP, any response made in a proposal should reference the applicable section numbers of this RFP.

3.1.2 PROPOSALS IN ENGLISH OR FRENCH

Proposals may be submitted in English or French.

3.1.3 NO INCORPORATION BY REFERENCE

The entire content of the proponent's proposal should be submitted in a fixed form, and the content of websites or other external documents referred to in the proponent's proposal but not attached will not be considered to form part of its proposal.

3.1.4 REFERENCES AND PAST PERFORMANCE

In the evaluation process, CMHC may include information provided by the proponent's references and may also consider the proponent's past performance or conduct on previous contracts with CMHC or other institutions.

3.1.5 INFORMATION IN RFP ONLY AN ESTIMATE

CMHC and its advisers make no representation, warranty or guarantee as to the accuracy of the information contained in this RFP or issued by way of addenda. Any quantities shown or data contained in this RFP or provided by way of addenda are estimates only, and are for the sole purpose of indicating to proponents the general scale and scope of the Deliverables. It is the proponent's responsibility to obtain all the information necessary to prepare a proposal in response to this RFP.

3.1.6 PROPONENTS TO BEAR THEIR OWN COSTS

The proponent will bear all costs associated with or incurred in the preparation and presentation of its proposal, including, if applicable, costs incurred for interviews or demonstrations.

3.1.7 PROPOSAL TO BE RETAINED BY CMHC

All proposals and related materials provided by the proponent shall, as of the Submission Deadline, become the sole property of CMHC and will not be returned to the proponent.

3.1.8 TRADE AGREEMENTS

Proponents should note that procurements falling within the scope of Chapter 5 of the Canadian Free Trade Agreement and/or Chapter 19 of the Canada-European Union (EU) Comprehensive Economic and Trade Agreement (CETA) are subject to that trade agreement but that the rights and obligations of the parties will be governed by the specific terms of this RFP.

3.1.9 NO GUARANTEE OF VOLUME OF WORK OR EXCLUSIVITY OF CONTRACT

CMHC makes no guarantee of the value or volume of Deliverables to be assigned to the successful proponent. The agreement to be negotiated with the selected proponent will not be an exclusive contract for the provision of the described Deliverables. In its sole discretion, CMHC may contract with others for goods and services that are the same as or similar to the Deliverables or may obtain such goods and services internally.

3.2 COMMUNICATION AFTER ISSUANCE OF RFP

3.2.1 PROPONENTS TO REVIEW RFP

Proponents should promptly examine all of the documents comprising this RFP and may direct questions or seek additional information in writing by email to the RFP Contact on or before the Deadline for Questions, pursuant to Section 1.4 of this RFP. No such communications are to be directed to anyone other than the RFP Contact. CMHC is under no obligation to provide additional information, and CMHC is not responsible for any information provided by or obtained from any source other than the RFP Contact. It is the responsibility of the proponent to seek clarification from the RFP Contact on any matter it considers to be unclear. CMHC is not responsible for any misunderstanding on the part of the proponent concerning this RFP or its process.

3.2.2 ALL NEW INFORMATION TO PROPONENTS BY WAY OF ADDENDA

This RFP may be amended only by addendum in accordance with this section. If CMHC, for any reason, determines that it is necessary to provide additional information relating to this RFP, such information will be communicated to all proponents by addendum. Each addendum forms an integral part of this RFP and may contain important information, including significant changes to this RFP. Proponents are responsible for obtaining all addenda issued by CMHC. In the Submission Form (Appendix B), proponents should confirm their receipt of all addenda by setting out the number of each addendum in the space provided.

3.2.3 POST-DEADLINE ADDENDA AND EXTENSION OF SUBMISSION DEADLINE

If CMHC determines that it is necessary to issue an addendum after the Deadline for Issuing Addenda, CMHC may extend the Submission Deadline for a reasonable period of time.

3.2.4 VERIFY, CLARIFY AND SUPPLEMENT

When evaluating proposals, CMHC may request further information from the proponent or third parties in order to verify, clarify or supplement the information provided in the proponent's proposal, including but not limited to clarification with respect to whether a proposal meets the mandatory technical requirements set out in Section I of the RFP Specifications (Appendix C). CMHC may revisit and re-evaluate the proponent's proposal or ranking on the basis of any such information.

3.3 NOTIFICATION AND DEBRIEFING

3.3.1 NOTIFICATION TO OTHER PROPONENTS

Once an agreement is executed by CMHC and a proponent, the other proponents will be notified of the outcome of the procurement process.

3.3.2 DEBRIEFING

Proponents may request a debriefing after receipt of a notification of the outcome of the procurement process. All requests must be in writing to the RFP Contact and must be made within sixty (60) days of such notification. The intent of the debriefing information session is to aid the proponent in presenting a better proposal in subsequent procurement opportunities. Any debriefing provided is not for the purpose of providing an opportunity to challenge the procurement process or its outcome. The debriefing will be provided in writing.

3.3.3 PROCUREMENT PROTEST PROCEDURE

If a proponent wishes to challenge the RFP process, it should provide written notice to the RFP Contact in accordance with the applicable trade agreement. The notice must provide a detailed explanation of the proponent's concerns with the procurement process or its outcome.

3.4 CONFLICT OF INTEREST AND PROHIBITED CONDUCT

3.4.1 CONFLICT OF INTEREST

CMHC may disqualify a proponent for any conduct, situation, or circumstances, determined by CMHC, in its sole and absolute discretion, to constitute a "Conflict of Interest", as defined in the Submission Form (Appendix A).

3.4.2 DISQUALIFICATION FOR PROHIBITED CONDUCT

CMHC may disqualify a proponent, rescind an invitation to negotiate or terminate a contract subsequently entered into if CMHC determines that the proponent has engaged in any conduct prohibited by this RFP.

3.4.3 PROHIBITED PROPONENT COMMUNICATIONS

Proponents must not engage in any communications that could constitute a Conflict of Interest and should take note of the Conflict-of-Interest declaration set out in the Submission Form (Appendix A).

3.4.4 PROPONENT NOT TO COMMUNICATE WITH MEDIA

Proponents must not at any time directly or indirectly communicate with the media in relation to this RFP or any agreement entered into pursuant to this RFP without first obtaining the written permission of the RFP Contact.

3.4.5 NO LOBBYING

Proponents must not, in relation to this RFP or the evaluation and selection process, engage directly or indirectly in any form of political or other lobbying whatsoever to influence the selection of the successful proponent(s).

3.4.6 ILLEGAL OR UNETHICAL CONDUCT

Proponents must not engage in any illegal business practices, including activities such as bid-rigging, price-fixing, bribery, fraud, coercion or collusion. Proponents must not engage in any unethical conduct, including lobbying (as described above) or other inappropriate communications; offering gifts to any employees, officers, agents, appointed officials or other representatives of CMHC; deceitfulness; submitting proposals containing misrepresentations or other misleading or inaccurate information; or any other conduct that compromises or may be seen to compromise the competitive process.

3.4.7 PAST PERFORMANCE OR PAST CONDUCT

CMHC may prohibit a supplier from participating in a procurement process based on past performance or based on inappropriate conduct in a prior procurement process with CMHC or any other organization, including but not limited to the following:

- illegal or unethical conduct as described above;
- the refusal of the supplier to honour its submitted pricing or other commitments; or
- any conduct, situation or circumstance determined by CMHC, in its sole and absolute discretion, to have constituted an undisclosed Conflict of Interest.

3.5 CONFIDENTIAL INFORMATION

3.5.1 CONFIDENTIAL INFORMATION OF CMHC

All information provided by or obtained from CMHC in any form in connection with this RFP either before or after the issuance of this RFP:

- is the sole property of CMHC and must be treated as confidential;
- is not to be used for any purpose other than replying to this RFP and the performance of any subsequent contract for the Deliverables;
- must not be disclosed to third parties without prior written authorization from the RFP Contact; and
- must be returned by the proponent to CMHC immediately upon the request of CMHC.

3.5.2 CONFIDENTIAL INFORMATION OF PROPONENT

A proponent should identify any information in its proposal or any accompanying documentation supplied in confidence for which confidentiality is to be maintained by CMHC. The confidentiality of such information will be maintained by CMHC, except as otherwise required by law or by order of a court or tribunal. Proponents are advised that as a Crown Corporation, CMHC is subject to the federal legislation with respect to access to information and privacy. Information submitted by third parties will be protected or may be required to be disclosed in specific circumstances pursuant to the federal legislation. Proponents are also advised that their proposals may, as necessary, be disclosed on a confidential basis, to CMHC's advisers retained to advise or assist with the RFP process, including the evaluation of proposals. If a proponent has any questions about the collection and use of personal information pursuant to this RFP, questions are to be submitted to the RFP Contact.

3.6 PROCUREMENT PROCESS NON-BINDING

3.6.1 NO CONTRACT A AND NO CLAIMS

This procurement process is not intended to create and will not create a formal, legally binding bidding process and will instead be governed by the law applicable to direct commercial negotiations. For greater certainty and without limitation:

(1) this RFP will not give rise to any Contract A–based concept or any other similar legal concepts or principles that may be applicable to the procurement process; and

(2) neither the proponent nor CMHC will have the right to make any claims (in contract, tort, or otherwise) against the other with respect to the selection of proponents, a decision to reject a proposal or disqualify a proponent, or a decision of the proponent to withdraw its proposal.

Notwithstanding the foregoing or anything to the contrary herein, CMHC's total liability to proponents for any cause of action arising out of or in relation to this RFP process, giving rise to liability, whether in contract or in tort, shall be limited to the reasonable costs incurred by proponents in preparing its proposal for matters relating to this RFP process. In no event, whether in contract or in tort shall CMHC be liable for any indirect, consequential, exemplary, punitive, incidental, or special damages or lost profits, even if CMHC has been advised of the possibility of such damages in advance.

3.6.2 NO CONTRACT UNTIL EXECUTION OF WRITTEN AGREEMENT

This RFP process is intended to identify prospective suppliers for the purposes of negotiating potential agreements. No legal relationship or obligation regarding the procurement of any goods or services will be created between the proponent and CMHC through this RFP process until the successful negotiation and execution of a written agreement for the acquisition of such goods and/or services.

3.6.3 NON-BINDING PRICE ESTIMATES

While the pricing information provided in proposals will be non-binding prior to the execution of a written agreement, such information will be assessed during the evaluation of the proposals and the ranking of the proponents. Any inaccurate, misleading, or incomplete information, including withdrawn or altered pricing, could adversely affect the evaluation or ranking or the decision of CMHC to enter into an agreement with the proponent for the Deliverables.

3.6.4 CANCELLATION

CMHC may cancel or amend the RFP process without liability at any time.

3.7 GOVERNING LAW AND INTERPRETATION

These Terms and Conditions of the RFP Process:

(1) are intended to be interpreted broadly and independently (with no particular provision intended to limit the scope of any other provision).

(2) are non-exhaustive and will not be construed as intending to limit the pre-existing rights of the parties to engage in pre-contractual discussions in accordance with the common law governing direct commercial negotiations; and

(3) are to be governed by and construed in accordance with the laws of the province of Ontario and the federal laws of Canada applicable therein.

[End of Part 3]

APPENDIX A – SUBMISSION FORM

Each proposal must include a Submission Form completed and signed by an authorized representative of the proponent.

1. PROPONENT INFORMATION

Please fill out the following form, naming one person to be the proponent's contact for the RFP process and for any clarifications or communication that might be necessary.	
Procurement Business Number (PBN):	
Full Legal Name of Proponent:	
Any Other Relevant Name under which Proponent Carries on Business:	
Street Address:	
City, Province/State:	
Postal Code:	
Phone Number:	
Company Website (if any):	
Proponent Contact Name and Title:	
Proponent Contact Phone:	
Proponent Contact Email:	

2. ACKNOWLEDGMENT OF NON-BINDING PROCUREMENT PROCESS

The proponent acknowledges that the RFP process will be governed by the terms and conditions of the RFP, 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 goods or services will be created between CMHC and the proponent unless and until CMHC and the proponent execute a written agreement for the Deliverables.

3. ABILITY TO PROVIDE DELIVERABLES

The proponent has carefully examined the RFP documents and has a clear and comprehensive knowledge of the Deliverables required. The proponent represents and warrants its ability to provide the Deliverables in accordance with the requirements of this RFP.

4. NON-BINDING PRICING

The proponent has submitted its pricing in accordance with the instructions in the RFP and in the Pricing Form (Appendix B). The proponent confirms that the pricing information provided is accurate.

The proponent acknowledges that any inaccurate, misleading or incomplete information, including withdrawn or altered pricing, could adversely impact the acceptance of its proposal or its eligibility for future work with CMHC.

5. ADDENDA

The proponent is deemed to have read and taken into account all addenda issued by CMHC prior to the Deadline for Issuing Addenda. The proponent is requested to confirm that it has received all addenda by listing the addenda numbers, or if no addenda were issued by writing the word "None", on the following line:_____. Proponents who fail to complete this section will be deemed to have received all posted addenda.

6. NO PROHIBITED CONDUCT

The proponent declares that it has not engaged in any conduct prohibited by this RFP.

7. CONFLICT OF INTEREST

For the purposes of this RFP, the term "Conflict of Interest" includes, but is not limited to, any situation or circumstance where:

(1) in relation to the RFP process, the proponent has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including but not limited to (i) having, or having access to, confidential information of CMHC in the preparation of its proposal that is not available to other proponents, (ii) communicating with any person with a view to influencing preferred treatment in the RFP process (including but not limited to the lobbying of decision makers involved in the RFP process), or (iii) engaging in conduct that compromises, or could be seen to compromise, the integrity of the open and competitive RFP process or render that process non-competitive or unfair; or

(2) in relation to the performance of its contractual obligations under a contract for the Deliverables, the proponent's other commitments, relationships, or financial interests (i) could, or could be seen to, exercise an improper influence over the objective, unbiased and impartial exercise of its independent judgement, or (ii) could, or could be seen to, compromise, impair or be incompatible with the effective performance of its contractual obligations.

For the purposes of section 7 (a)(i) above, proponents should disclose the names and all pertinent details of all individuals (employees, advisers, or individuals acting in any other capacity) who (1) participated in the preparation of the proposal; **AND** (2) were employees of CMHC within twelve (12) months prior to the Submission Deadline. Any former public office holder must be in compliance with the post-employment provisions of the Conflict of Interest and Post-Employment Code for Public Office Holders (2012) in order to derive a direct benefit from any contract which may arise from this RFP.

If the box below is left blank, the proponent will be deemed to declare that (1) there was no Conflict of Interest in preparing its proposal; and (2) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the RFP.

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

The proponent declares that there is an actual or potential Conflict of Interest relating to the preparation of its proposal, and/or the proponent foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the RFP.

If the proponent declares an actual or potential Conflict of Interest by marking the box above, the proponent must set out below details of the actual or potential Conflict of Interest:

_____

_____

8. DISCLOSURE OF INFORMATION

The proponent warrants that neither the proponent nor one or more of the proponent's directors, officers or employees have been convicted or sanctioned for an offence involving bribery, corruption, or workplace safety at any time. If such convictions exist, the details of such convictions or sanctions are to be disclosed in the proponent's proposal.

It is understood that CMHC will have the sole discretion to determine whether such convictions are grounds for removing the proponent from further consideration in the RFP process or requiring that the proponent exclude certain employees from involvement in the provision of goods and/or services contemplated herein.

The proponent 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 proponent hereby consents to the disclosure, on a confidential basis, of this proposal by CMHC to the advisers retained by CMHC to advise or assist with the RFP process, including with respect to the evaluation this proposal.

9. SECURITY CLEARANCE

The proponent agrees that it and any other persons for which it is responsible, who are to perform the work as stated in this RFP, at the request of CMHC will comply with security screening as outlined in Section E. Security of the RFP Specifications (Appendix C).

Signature of Witness	Signature of Proponent Representative
Name of Witness	Name of Proponent Representative
	Title of Proponent Representative
	Date
	I have the authority to bind the proponent.

APPENDIX B – PRICING FORM

1. INSTRUCTIONS ON HOW TO COMPLETE PRICING FORM

Rates must be provided in Canadian funds, inclusive of all applicable duties and taxes except for HST**,** which should be itemized separately.

Rates quoted by the proponent must be all-inclusive and must include all labour and material costs, on-going maintenance costs, all travel and carriage costs, all insurance costs, all costs of delivery (including any on-boarding/training costs, if not listed separately in the pricing form), all costs of installation and set-up, including any pre-delivery inspection charges, and all other overhead, including any fees or other charges required by law.

Travel expenses are considered separate expenses and will be reimbursed in accordance with CMHC's Travel Policy outlined in the Form of Agreement included in Appendix A of this RFP.

2. EVALUATION OF PRICING

Pricing is worth 30% points of the rated criteria score.

The sub-total of Table 1, Table 2, and Table 3 will be combined to obtain the pricing that will be scored based on a relative pricing formula using the rates set out in the Pricing Form. Each proponent will receive a percentage of the total possible points allocated to price for the particular category it has bid on, which will be calculated in accordance with the following formula:

Lowest price ÷ proponent's price x weighting = proponent's pricing points

3. PRICING FORM

Table 1 – Deliverables (Initial Term – 3 years)

ITEM No	DELIVERABLE	DESCRIPTION	QTY	UNIT COST	TOTAL CDN BEFORE TAX
1	Implementation Costs	One-time cost for requirements gathering, deployment scoping, configuration, and implementation.			
2	Data Migration	One-time cost for complete migration of audit data from TeamMate+, including configuration and testing.			
3	Annual Fees	Complete detailed description of the licensing costs per module (if applicable) for 200 risk & audit user licenses.			
4	On-going support costs	Annual cost of on-going maintenance and support services per licence for 200 risk & audit user licenses, if not included in Item 2 Annual Fees.			
5	Training Costs	Cost that cover: 1. On-line (self-taught) 2. On-line instructor led			
6	Other				
7	Other				
8	Other				
SUB-TOTAL (this value will be used for the evaluation of pricing)					

Blank rows (Item # 6-8) are provided in the table above for proponents to include any additional items ("Other") which they intend to charge for during the Initial Term of the Agreement. All Other costs will form part of the subtotal and the proponent's evaluated price.

Table 2 – Deliverables (Optional Renewal Terms – Year 4-5)
Please insert pricing for the two annual renewal option years including the Items from Table 1, as applicable.

Table 3 – Professional Services
Please insert pricing in the following table for the hourly rate for professional services. Professional services will be provided on an as-and when required basis. The rate must be firm for the Initial Term.

ITEM No	DELIVERABLE	DESCRIPTION	ANNUAL QTY*	HOURLY RATE	TOTAL CDN BEFORE TAX
1	Professional Services	Professional services for requirements not included in the initial requirements, for example: in the event of a new configuration or expansion of the solution, consulting services, etc.	30		
2	Product Upgrade Support	Professional services for product upgrade support, specially to facilitate the testing of new functionality and ensure regression testing has been completed on CMHC's configurations.	30		
SUB-TOTAL (this value will be used for the evaluation of pricing)					
*QTY: Estimated quantity of hours to be used by CMHC for evaluation purposes only.					

Table 4 – Optional Additional Deliverables
Please insert pricing in the following table for the optional additional Modules. The Unit Cost must be firm for the Initial Term.

ITEM No	DELIVERABLE	DESCRIPTION	QTY	ANNUAL LICENCE COST	TOTAL CDN BEFORE TAX
0	Optional Additional Services	Licensing fees per Use Cases Cost and structure of licensing for additional modules, if required, after implementation due to expansion of employee base.	N/A	N/A	N/A
1		ERM, RAS and Metrics			
2		IT & Security Risk Management			
3		Vendor Risk Management			
4		Crisis & BCM Risk Management			
5		ESG Risk Management			
6		Model Risk Management			

7	Other				
8	Other				
9	Other				

Blank rows (Item # 7-9) are provided in the table above for proponents to include any additional items/costs (“Other”) related to the purchase and implementation of optional additional modules.

APPENDIX C – RFP SPECIFICATIONS

A. SCOPE OF WORK AND DELIVERABLES

CMHC is seeking a cloud-based Software as a Service (SaaS) solution for Governance, Risk and Compliance (GRC). The proposed solution must initially include the module(s) to meet the following use cases:

- General Functionality
- Operational Risk
- Compliance
- Internal Controls
- Internal Audit
- Metrics and Reporting

"Use Cases" are defined as software capabilities that allow business users to perform tasks to achieve specific goals.

The solution must have the ability to expand to add the module(s) to meet the following additional use cases if requested by CMHC in the future (e.g.: vendor risk, IT risk, BCM risk, etc.):

- IT Risk and Security
- Model Risk Management
- Risk Appetite, ORSA and ERM
- Vendor Risk Management
- Business continuity management (BCM) and disaster recovery planning (DRP)
- ESG Management

Services are to include software, technical support, consultation, training, customization, testing, data migration, installation, implementation, and on-going maintenance services.

The selected proponent must provide to CMHC the following deliverables:

1. A cloud-based system that supports all requirements listed in Sections H. Mandatory Technical Requirements and R.5 Functional Requirements of this Appendix;
2. A support service to handle issues encountered during the term of the resulting agreement (including optional renewal terms);
3. A complete plan for implementation, including milestone schedule, deliverable dates, and support;
4. A complete plan for training users and super users (administrators of the system). The selected proponent will be responsible for implementing the training plan, providing the training to CMHC staff, and providing all training material.
5. The complete migration of all existing historical audit project files from legacy audit management system (TeamMate+) to the selected proponent's proposed SaaS Solution.

B. WORK LOCATION

The work will be performed at the selected proponent's place of business.

C. TRAVEL

No travel is required in the course of the contract and no compensation will be awarded to the selected proponent for any travel cost incurred.

D. SECURITY

Employees of the proponent and, if applicable, subcontractors may be required to undergo a criminal records check and must hold a valid personnel security screening at the level of **RELIABILITY clearance** prior to commencement of any work under the Agreement and must provide the results of the check to CMHC's corporate security department. CMHC reserves the right to disallow any person to carry out work under the Agreement on the basis of the results of the criminal records check/security clearance.

Each of the proponent's proposed staff or subcontractors, who do not hold a valid clearance, will be required to complete a "Security Clearance Form" (67934) upon request from CMHC.

E. CMHC DATA

The purpose of this section is to set out the proponent's obligations in respect of the technology, the property, CMHC intellectual property rights, CMHC developments and/or CMHC confidential information ("CMHC Data") residing on the proponent's network or for which the proponent has access, custody or control. The proponent shall:

The proponent shall store CMHC Data in Canada at all times and data in transit shall not cross any international borders for any reason including the United States. Data at rest and in transit shall be protected and encrypted at all times.

In addition to being security cleared, each of the proponent's staff or subcontractors who work on this project must access CMHC data (including access for the purpose of technical, implementation and operational support) from Canada or countries where Canada has a bilateral agreement on security.

The proponent must show validation they have security controls in place to safeguard data up to and including Protected B.

Protected B information includes information that if compromised could cause significant injury, such as significant financial loss, identity theft, loss of reputation or competitive edge, to an individual or CMHC. It includes:

- Financial and risk related Information
- Internal CMHC procedures that are not publicly available
- Security controls

F. MATERIAL DISCLOSURES

Intentionally Deleted.

G. MANDATORY SUBMISSION REQUIREMENTS

SUBMISSION FORM (APPENDIX A)

Each proposal must include a Submission Form (Appendix A) completed and signed by an authorized representative of the proponent.

PRICING FORM (APPENDIX B)

Each proposal must include a Pricing Form (Appendix B) completed according to the instructions contained in the form.

H. MANDATORY TECHNICAL REQUIREMENTS

Proponents must provide a statement per each Mandatory Technical Requirement ("MTR") as to how the proponent is in compliance with the MTR outlined in the table below. The following MTR will be assessed on a pass/fail basis:

#	MTR Description	Proponent Confirmation (Page # in proposal)
MTR.1	Infrastructure: The system must be hosted on or able to be hosted on cloud based infrastructure. The system must be completely provided as a Software as a Service (SaaS).	
MTR.2	Data Residency: The system must store all data at rest in Canada at all times (data must reside in Canada during all stages of all processes).	
MTR.3	Security and Access Management: The system must have the ability to manage user access through profiles, roles, and groups.	
MTR.4	Integration: The system must have the capability to integrate to other applications (i.e. active directory, ticketing system, security incident management (SIMS) application, authoritative sources, etc.).	
MTR.5	Configuration Flexibility: The system must be configurable and CMHC administrators must be able to configure key elements (e.g., views, taxonomies, assessments, workflows, etc.).	
MTR.6	Audit Capability: The system must have the capability for audit trail and history capture (at least 24 months) and reporting of the rating changes and other assessment changes.	
MTR.7	Common Risk Assessment Requirements: The system must support performing various types of risk assessment, including enterprise top-down and bottom-up, risk self-assessments, ability to normalize and aggregate risks, analyze risks, and report on risk profile.	
MTR.8	Common Risk Assessment Requirements: The system must allow for many-to-many relationships to be established between foundational data elements such as processes to risks, risks to controls, loss events to risks, etc.	
MTR.9	Common Risk Assessment Requirements: The system must allow assessment of inherent and residual risk using qualitative assessment criteria (i.e., high, medium, low).	
MTR.10	Common Risk Assessment Requirements: The system must have the capability to identify and assess (using standard rating matrix) the risks related to the activities, processes, and deliverables of an area being assessed.	
MTR.11	Common Risk Assessment Requirements: The system must have the capability to document audit project risk assessment and link to corporate enterprise risks.	
MTR 12	Availability: The system must be available at a commercially reasonable response time (99.9% of the time during hours of availability over a month).	
MTR 13	Disaster Recovery: The proponent must maintain a Disaster Recovery Plan to support its ability to deliver technology services through disruption.	
MTR 14	The Solution must be an out of the box tool that is currently in use in the market. CMHC is not considering a custom-built solution. The modules to enable the selected uses cases should be fully integrated and should not require customization.	

I. PRE-CONDITIONS OF AWARD

A proponent invited to enter into direct contract negotiations should be prepared to: (i) satisfy the pre-conditions of award listed in this Section I. If the pre-conditions of award are not satisfied within the contemplated Contract Negotiation Period, pursuant to Section 1.4 of this RFP, then CMHC may discontinue negotiations with the top-ranked proponent and invite the next-best-ranked proponent to enter into negotiations.

A. Security Clearance Verification of Proposed Resources

In accordance with Appendix C, Section B. Security, the selected proponent shall provide the following for CMHC's Security department to verify the proposed resources hold valid security clearances:

Personnel Security Clearance:

Resource Name	Security Clearance Level	Security Clearance Number	Clearance Validity Period

B. References

CMHC may conduct a reference check. The references provided must be deemed successful by CMHC. If the proponent fails, such reference check it may be disqualified from further consideration.

C. Proof of Insurance

In accordance with Article 13 (Insurance Obligations) outlined in Appendix D – Form of Agreement, the selected proponent shall procure and maintain, at its own expense, insurance coverage in force for the duration of the Agreement, as evidenced by the Certificate of Insurance.

The selected proponent shall furnish CMHC with original Certificates of Insurance including all required amendatory endorsements (or copies of the applicable policy language effecting coverage required by Article 13) and a copy of the Declarations and Endorsement Page of the CGL policy listing all policy endorsements to CMHC before work begins. CMHC reserves the right to require certified copies of all insurance coverage and endorsements.

If the selected proponent is not able to comply with the insurance requirements, it may not be awarded an agreement.

D. Privacy and Security Controls Questionnaire (Appendix E)

The selected proponent will provide a completed copy of the Appendix E Privacy and Security Controls Questionnaire demonstrating compliance with the requirements in the Form of Agreement. If the selected proponent is not able to comply with the requirements, it may not be awarded an agreement.

E. Business Continuity and Disaster Recovery Attestation Form (Appendix F)

The selected proponent will provide a completed copy of the Appendix F Business Disaster Recovery Attestation Form demonstrating compliance with the requirements in the Form of Agreement. If the selected proponent is not able to comply with the requirements, it may not be awarded an agreement.

J. RATED CRITERIA

The following sets out the categories, weightings, and descriptions of the rated criteria of the RFP.

<table>
<tr><th>Rated Criteria Category</th><th>Weighting (%)</th></tr>
<tr><td>R.1 Experience and Qualifications of the Organization</td><td>5%</td></tr>
<tr><td>R.2 Approach and Methodology</td><td>5%</td></tr>
<tr><td>R.3 Experience and Qualification of the Proposed Resource(s)</td><td>5%</td></tr>
<tr><td>R.4 Functional Requirements – Weighting Breakdown
<table>
<tr><th>ID #</th><th>Rated Criteria</th><th>Weighting</th></tr>
<tr><td>4.1</td><td>General Functionality</td><td>17%</td></tr>
<tr><td>4.2</td><td>Metrics and Reporting</td><td>10%</td></tr>
<tr><td>4.3</td><td>Operational Risk</td><td>15%</td></tr>
<tr><td>4.4</td><td>Internal Audit</td><td>15%</td></tr>
<tr><td>4.5</td><td>Risk Appetite, ORSA and ERM</td><td>3%</td></tr>
<tr><td>4.6</td><td>Compliance</td><td>15%</td></tr>
<tr><td>4.7</td><td>Internal Controls</td><td>10%</td></tr>
<tr><td>4.8</td><td>Vendor Risk Management</td><td>3%</td></tr>
<tr><td>4.9</td><td>IT Risk and Security</td><td>3%</td></tr>
<tr><td>4.10</td><td>Business Continuity Management (BCM) and Disaster Recovery Planning (DRP)</td><td>3%</td></tr>
<tr><td>4.11</td><td>Model Risk Management</td><td>3%</td></tr>
<tr><td>4.12</td><td>Environmental, Social, and Governance (ESG) Management</td><td>3%</td></tr>
<tr><td></td><td>Total (40%)</td><td>100%</td></tr>
</table></td><td>40%</td></tr>
<tr><td>K. Presentations</td><td>15%</td></tr>
<tr><td>Stage III - Pricing (See Appendix B for details)</td><td>30%</td></tr>
<tr><td>Total</td><td>100%</td></tr>
</table>

Submission requirements (proposal content) for each rated criteria category

Note:

Each proponent should provide the following in its proposal in the same order as listed below. Page limitations are per single-sided pages, minimum font size 11.

R. 1 EXPERIENCE AND QUALIFICATIONS OF THE ORGANIZATION

R.1.1 Provide a brief description of your organization (overview and history).

R.1.2 Describe your product roadmap with respect to incorporating emerging technologies, including AI, predictive analytics, and machine learning.

R.1.3 Describe in detail the organization's expertise in the applicable fields relevant to scope of work. The response should include information on:

a) Years of experience in the field of Governance, Risk and Compliance SaaS Solutions;

b) Breadth of experience in the field of Governance, Risk and Compliance SaaS Solutions;

R.1.4 Range of clients in the field of Governance, Risk and Compliance SaaS Solutions. Include at least two (2) public agencies, and large complex organizations such as financial institutions and/or mortgage insurers..

R.1.5 Please describe how CMHC will benefit from your organization's expertise outlined under R.1.3 a) and b) and R.1.4.

R.1.6 Please provide two (2) examples of work performed for other clients similar to the requirements set out in the Deliverables of the RFP.

R.1.7 Provide SOC Reports for last three (3) years.

R.1.8 Disaster Recovery Plan:

a) Detail your organizations recovery time and recovery point objectives. Include the frequency the Disaster Recovery (DR) Systems are tested and confirm testing is in accordance with client agreed upon RTO.

b) The proponent must maintain an Enterprise Disaster Recovery Framework (EDRF) to support its ability to deliver technology services through disruption. EDRF as per defined in OSFI Guideline B13 Technology and Cyber Risk Management section 5.1 5.1 Disaster Recovery.

R.1.9 Business Continuity Plan – Detail your Organization's Business Impact Analysis (BIA) and Business Continuity Plan (BCP) and the frequency they are updated. Include the frequency the BCP is exercised including a description communications strategy, critical contact names, etc.).

R.1.10 Diversity and Inclusion:

a) Indicate whether you have a supplier diversity program in place.
b) Indicate whether your organization considers itself a diverse supplier. A diverse supplier is defined as an organization that is owned and controlled by at least 51% of individual(s) who are considered: women, indigenous people, LGBTQ2+, persons with disabilities and visible minorities. If so, indicate whether your organization is a certified diverse supplier and provide certification details.

R.1.11 Proponent's Organizational Information:

a) Describe internal ethics policies and procedures including how violations are documented and reported.
b) Indicate the location of your data centers and back up / recovery centers and if they are in a single or multiple locations. Include information on locations in disaster prone areas.

c) Indicate current environmental initiatives and corporate environmental policies and procedures demonstrating responsible environmental stewardship and any associated targets and if renewable power sources are used for data centers.

R. 2 APPROACH AND METHODOLOGY

R.2.1 Describe why your organization is ideally suited to provide the Deliverables to CMHC.

R.2.2 Outline how CMHC's account would be handled by your organization to ensure that it receives cost-effective, prompt, personal, efficient, and high-quality service.

R.2.3 Describe how you will meet all CMHC requirements set out in Appendix C.

R.2.4 Provide a description of governance models used for similar engagements.

R.2.5 Describe what in-house support your organization offers for implementation, for example, implementation partners, advisors, and consultants).

R.2.6 Describe your organizations approach to continuous improvement with respect to products and service offerings?

R.2.7 Describe services and/or business functions that will be sub-contracted under any resulting agreement. Provide sub-contractor name, contract information, and roles and responsibilities assigned to a sub-contractor.

R.2.8 Describe how often the system is upgraded and how much time is given to customers to adopt new versions. Detail how long support is provided for previous versions and the quantity of previous versions that are supported.

R.2.9 Provide your End of Support/ End of Life Policy.

R.2.10 Detail the past outage experience for the past two (2) years, including:

a) Frequency and duration of system outages; and

b) The duration required to successfully complete critical repairs.

R.2.11 A smooth and orderly transition from the existing TeamMate+ system to the selected proponent's solution to assure minimum disruption to CMHC activities is critical. The proponent shall describe its:

a) Experience in previous migrations, including accuracy in previous migrations. What percentage of the services required corrections?
b) Transition plan including a strategy for migrating all catalogue items, configuring the system to match the categories, landing pages, etc., and implementing all functions.
c) Recommended approach for CMHC to avoid operational disruptions during the transition.

R. 3 EXPERIENCE AND QUALIFICATIONS OF THE PROPOSED RESOURCES

R.3.1 Name the key representative(s) for the CMHC account and provide his/her qualifications.

R.3.2 Provide a brief bio and qualifications (one page per resource) of the resources assigned to applicable areas of expertise.

R.3.3 Briefly describe the role and level of involvement of the key resources in the examples described under R.1.4 and R.1.6 above.

R. 4 FUNCTIONAL REQUIREMENTS

See Annex 1 to this Appendix C for a detailed list of the functional requirements.

K. PRESENTATION

The purpose of the Presentation is to allow: (a) the qualified proponents to address the major elements of their proposal, (b) the Evaluation Team to obtain any required clarification based on a set of pre-defined questions, which will be issued by CMHC, and (c) the members of the Evaluation Team to interact directly with key representatives of the proponent's proposed team.

In advance of the Presentation, each proponent invited to make the Presentation will receive in writing: (i) the agenda for the Presentation and (ii) a set of pre-defined questions that they will be required to address in their Presentation. The Presentation will occur via video conferencing.

The Presentation has an assigned weighting of 15% and will be evaluated as per the following:

Presentation Rated Criteria		**Weighting (%)**
1.0	Presentation of proponent's proposal and answers to pre-defined questions	30 %
2.0	Demonstration of specific use cases (demonstrating the tool can provide the desired output) and ease of configuration	30 %
3.0	Ease of use (navigation is intuitive) for business needs	40 %
Total (15%)		100%

L. REFERENCES

Each proponent is requested to provide three (3) references from clients who have obtained goods or services similar to those requested in this RFP from the proponent within the five (5) previous years of the issuance of this RFP.

CMHC may contact these references as per Section 3.1.4 References and past performance (Part 3 -Terms and Conditions of the RFP Process) and/or as per Section I. Pre-conditions of Award (Appendix C – RFP Specifications).

ANNEX 1 TO APPENDIX C – FUNCTIONAL REQUIREMENTS (R4)

The Functional Requirements Submission must provide sufficient yet concise information to reasonably demonstrate that the proponent's proposed SaaS Solution (the "System") can meet the responsibilities and obligations as set out in the Form of Agreement. When responding, the Proponent must identify requirements that are not currently being offered by the Proponent to other clients.

Rated ID	Description	Weighting	Proponent Response (This column is provided for the Proponent to include their response to the Functional Requirement)
4.1	**General Functionality** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's general functionality requirements.	**17%**	
4.1.1	**General Requirements (languages, attachments, archiving)** The Proponent must respond by describing how their System allows for the following general requirements:		
a	The System allows screens to be represented in English and French. The System should allow data to be entered in multiple languages (English and French).	**3**	
b	The System should allow for attachments to be uploaded into specific fields within specific records and for SharePoint links to be added to specific fields.	**3**	
c	The System should allow data to be archived on a periodic (quarterly/annual) basis.	**3**	
d	The System should have the ability to display multiple time zones based on location.	**2**	
e	The System should allow keyword search functionality across the System.	**2**	
4.1.2	**System Maintenance and Support** The Proponent must respond by detailing their customer support offerings and the System maintenance processes referencing the following:		
a	The Proponent should provide support offerings during business hours (EST hours) and Proponent should provide appropriate severity levels for support issues with clear SLAs for response and escalation process.	**3**	

b	The Proponent should provide training material for out of the box navigation including but not limited to user guides, quick reference materials, FAQs, and end user training videos.	**3**	
c	Platform Updates: The system must have a technology change and release management process and supporting documentation to ensure changes to technology assets are documented, assessed, tested, approved, implemented, and verified in a controlled manner that minimizes disruption to the production environment.	**3**	
4.1.3	**Performance and Scalability** The Proponent must respond by describing the System's performance and detailing its scalability referencing the following:		
a	The System should have mobile device compatibility for certain functionality (e.g., dashboard views).	**2**	
b	The System should be able to capture and report on statistics regarding system's downtime.	**2**	
c	The System should support a high volume of simultaneous users (minimum of 1000) in concurrent sessions without slowing down response time (assuming appropriate hardware in use).	**2**	
4.1.4	**Data Feeds and System Integration** The Proponent must respond by describing the System's data feeds and system integration capabilities referencing the following:		
a	The System should have the ability to ingest data feeds from risk alerts services.	**3**	
b	The System must have the ability to integrate to other applications (i.e., ticketing system, security incident management (SIMS) application, authoritative sources, etc.). These systems include: Qualys Vulnerability Management, Service Now, Kiteworks, Microsoft Defender, Microsoft Sentinel and Microsoft Active Directory.	**3**	
c	The System should provide the ability for import and export data in open standard format for import by applications (CSV, XLS, XML, DOC, HTTP, TXT, etc.).	**3**	
d	The System should provide the ability to interface with other systems and applications (i.e., MS Teams, SharePoint, Active Directory, Outlook, MS Excel, MS Power BI, etc.).	**3**	

4.1.5	**System Security** The Proponent must respond by describing the System's security features and capabilities referencing the following:		
a	The System should support ability to maintain privilege and privacy requirements for certain records (legal requirement).	**3**	
b	The System should enforce segregation of duties based on pre-defined rules and access roles (e.g., individual should not be able to approve their own requests).	**3**	
c	The System should support single sign-on integration capabilities.	**3**	
d	The System should support multi-factor authentication capabilities.	**3**	
e	The System should provide an out of the box user authentication mechanism.	**3**	
f	The System should provide security rules to protect direct access to client's data from the back end.	**3**	
g	The System should provide the ability to report on user access/activity.	**3**	
h	The System should provide the ability for users to change their own passwords.	**2**	
i	The System should provide the ability to lock out user access after a number of failed attempts.	**3**	
j	The System should provide the ability to encrypt passwords.	**3**	
k	The System should provide the ability to allow the system's control features to be reviewed by an independent auditor.	**3**	
l	The System should provide the ability to enforce security via HTTPS (SSL).	**3**	
m	The System should provide the ability to secure sensitive data from unauthorized users via database encryption.	**3**	
4.1.6	**Flexibility and Configuration** The Proponent must respond by describing the System's ease of use, including System flexibility and configuration referencing the following:		

a	The System presentation layer should be easily configurable to corporate types of root causes (at least 6) and impact (at least 6).	**3**	
4.1.7	**System Audit Tracking and Reporting** The Proponent must respond by describing the System's audit tracking and reporting capabilities referencing the following:		
a	The System should provide the ability to perform searches across the System's audit logs.	**2**	
b	The System should provide the ability to write and protect secure audit trails/logs. Audit logs must be maintained for at least 2 years.	**3**	
4.1.8	**Common Functionality Requirements** The Proponent must respond by describing the System's common functionality capabilities referencing the following:		
a	The System should provide the ability to track accountability and escalation processes.	**2**	
b	Ability to re-assign or delegate a task.	**3**	
c	The System should allow for approved users to designate ad-hoc approvers.	**2**	
d	The System should have ability for users to define and maintain a risk register and risk universe based on recognized standard (e.g.: COSO ERM Framework).	**3**	
E	Perform multi-layered risk assessments (i.e., enterprise level, business unit level, process level, etc.)	**2**	
f	Ability to generate a current risk profile at different levels in the organization hierarchy (i.e., business unit, regulation, category of risk, severity of risk and others).	**3**	
g	Ability to aggregate and /or filter risks based on configurable criteria.	**3**	
h	The System should be able to display historical versions of an object (i.e., risk rating, exception, etc.).	**2**	
i	The System should have the ability to display pre-set help text to assist users.	**3**	

j	The System should have the ability to create issues directly from a workflow.	**3**	
k	The System should provide a dashboard specific to the user logged in with "To Do's" and key attributes such as due date, action needed, and title of the record.	**3**	
l	The dashboards should contain hyperlinks that take the user directly to the record with pending action or easily navigate between records and attachments.	**3**	
4.1.9	**Notifications** The Proponent must respond by describing the System's notification capabilities referencing the following:		
a	The System should provide the ability to trigger notifications within the System and via e-mail based on conditions within records or by pre-set schedules.	**3**	
b	The System should provide the ability to have multiple notification templates	**2**	
c	The System should provide the ability to link into a record from within a notification.	**3**	
4.2	**Metrics and Reporting** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's metrics and reporting requirements.	**10%**	
4.2.1	**Quantification Engine** The Proponent must respond by describing the System's quantification engine capabilities referencing the following:		
a	The System should provide a basic set of quantification operators (+, -, *, /).	**3**	
b	The System should provide an intermediate set of mathematical operators (Sum, Average, Min, Max).	**3**	
c	The System should provide an advanced set of mathematical operators (Square Root, Ceiling, Standard Deviation, etc.).	**2**	
d	The System should provide logic statements to combine with mathematical operators (If, Then, Else, And, OR).	**3**	

e	The System should allow the use of user identities (names, groups, etc.) within the logic and mathematical quantification engine.	**3**	
f	The System should provide the ability to use time and date information within the logic and mathematical quantification engine.	**3**	
g	The System should be able to perform calculations to create statistical/operational reporting.	**3**	
4.2.2	**Basic Reporting** The Proponent must respond by describing the System's basic reporting capabilities referencing the following:		
a	The System should include a library of standard reports, such as: • Inherent and residual Risks by risk category, sector, product, etc. • Assurance Map of all activities planned/performed by each oversight functions with flexibility for various views (e.g., by risk category, process, business area, etc.). • Issue resolution/ management actions listing of all action plans across all oversight functions. • Risk and control matrix. • Project status, metrics, etc. Time tracking / resource management reporting".	**2**	
b	Reports should be available in a dynamic, drill down format.	**3**	
c	The System should provide ad hoc reporting capabilities and ability to customize reports and dashboards for specific needs.	**3**	
d	The Systems should provide multiple report delivery options e.g., scheduled, email attachment, link, embedded within the System, etc.	**2**	
e	Provide reports that display data in a graph or pictorial format.	**3**	
f	The System should be able to report on any data fields across multiple tables or applications (ex. for audit or a risk assessment - a report showing risks assessed, control results, residual risk, conclusions, etc.).	**3**	
g	The System should provide an easy and intuitive end-user interface to create reports.	**3**	

h	The System should have the capability for the business user to personalize dashboards or views, such as: - Individual assignments - Project and object progress	**3**	
i	The System should provide the ability to save reports as personal, group or public/global reports and as different templates (e.g., one template for Line of Business (LoB) A and another for LoB B, etc.).	**2**	
j	The System should provide the ability to schedule the delivery of reports at user specified times.	**2**	
4.2.3	**Metrics, KPIs, KRIs, Thresholds and Trends** The Proponent must respond by describing the System's metrics, KPI, KRI, thresholds, and trends capabilities referencing the following:		
a	The System should provide the ability to calculate/track ratings and metrics and key performance indicators information. System should allow tracking at least the following information: title, metric value, target value and various types of limit thresholds.	**3**	
b	The System should provide the ability to track for each KRI an absolute lower limit, lower tolerance, appetite lower limit, target, appetite upper limit, tolerance upper limit and absolute upper limit.	**3**	
c	The System should provide the ability to configure KPI /KRI record structure and calculations to include required data fields (control name, type, description, etc.).	**3**	
d	The System should provide the ability to manually input KPI /KRI data.	**3**	
e	The System should provide the ability to assign thresholds to risk level, loss value, number of events, date of events and notification when those thresholds are reached or exceeded.	**3**	
4.3	**Operational Risk** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's operational risk requirements.	**15%**	
4.3.1	**OpRisk - General Requirements** The Proponent must respond by describing the System's OPRisk capabilities referencing the following:		

a	Users should have the option to begin navigating through the System at any level of any hierarchy (business, business objective, asset, risk, control, etc.) and then navigate through the hierarchy up or down and jump hierarchies (e.g., control to risk).	**3**	
b	The System should allow risks to be associated to relevant objects, such as: objectives, sector, risk type, risk appetite level, assessment type, root cause type, impact type, processes, controls, regulations, sectors, policies, products/programs, systems, incidents, and remediation actions.	**3**	
c	The System should provide the ability to support multiple hierarchies to reflect business hierarchy, asset hierarchy, sector hierarchy, etc.	**3**	
d	The System should provide the ability to support a broad volume of changes (between 0 - 100) to multiple hierarchies annually either over the course of the year or at one time through a batch update.	**3**	
e	The System should provide the ability to support changes to the risk framework.	**2**	
4.3.2	**Risk Profiling** The Proponent must respond by describing the System's risk profiling capabilities referencing the following:		
a	The System should provide the ability to generate risk profiles for all entities of any hierarchy, a corresponding accountability matrix (may be metadata of the entity) and reporting from an entity view across any number of entity levels (Enterprise, sector, LoB, functional, process, asset views - and profiles at each level).	**3**	
b	The System should provide the ability to have a composite risk rating that can be calculated based off assessments, issues, incidents (Loss), KRIs, etc. by entity or at a risk profile level - roll-up of residual risk rating from assessments, issues, metrics (KRIs), scenario analysis, risk appetite and tolerance, etc.	**3**	
c	The System should provide the ability to change risk profiles based on changes to entity and quarterly or annual reviews of profile with sign-off/attestation.	**3**	
4.3.3	**Assessments** The Proponent must respond by describing the System's assessment capabilities referencing the following:		

a	The System should provide the ability to generate risk or control self-assessments and surveys and to use "assessment" functionality on a broader basis for information gathering.	**3**	
b	Ability to track and plan periodic re-validation Scheduling (Work Plan Development).	**3**	
c	The System should have functionality out of the box to support business entity level assessment surveys.	**3**	
d	The System should have functionality out of the box to conduct other risk assessment surveys (i.e., process, application, vendor, product, etc.).	**3**	
e	The System should have functionality out of the box to conduct New / modified Product risk assessments.	**3**	
f	The System should provide the ability to track assessment progress as a percentage complete or number of questions completed.	**3**	
g	The System should provide the ability determine type of answer expected (numeric, text, length, etc.).	**2**	
h	The System should provide the ability to dynamically (real time) show or hide questions based on answers to other questions.	**3**	
i	The System should provide the ability to support multiple workflows within the same assessment.	**2**	
j	The System should provide the ability to generate assessment scores based on numbers of right vs. wrong answers, as well as the ability to score based on question and answer weight.	**3**	
k	The System should be able contain a multi-level **risk hierarchy or taxonomy**, with a minimum of 4 levels of risk in the hierarchy with the ability to enforce either one to many or many to many associations between levels.	**3**	
l	The System should be able contain a multi-level **process hierarchy or taxonomy**, with a minimum of 4 levels of in the hierarchy with the ability to enforce one to many associations between levels.	**3**	
m	The System should provide the ability to store control testing procedures, guidance, and testing evidence for assessments and show their associations to other hierarchies (i.e., control, risk, asset, etc.).	**3**	
n	The System should have the ability to generate or associate assessments with loss event records, KRIs and issues.	**3**	

o	The System should have the ability for assessment scheduling (annual, quarterly, etc.), notifications and tracking.	**2**	
p	The System should provide the ability to generate assessments based on triggers such as KRI thresholds, findings/issues, self-identified due to changes in entity risk profiles.	**2**	
q	The System should provide the ability to manually override any calculated risk rating and capture a justification for the override (override may be in another field, all downstream calculations must user override if present).	**3**	
r	The System should provide the ability to roll risk ratings or scores up across multiple (associated) hierarchies, with no restrictions on the number of levels the risk rating or score can be rolled up through.	**3**	
s	The System should provide the ability to apply mathematical operators such as sum, average, ceiling, floor, min, max, etc. on risk ratings at any single level of a hierarchy or across multiple levels of a hierarchy.	**2**	
t	The System should provide the ability to perform 2-step risk assessments where the 1st line users can identify a risk and perform a draft assessment before transitioning it over to the 2nd line for validation and analysis	**3**	
4.3.4	**Findings and Issues Management** The Proponent must respond by describing the System's findings and issue management capabilities referencing the following:		
a	The System should provide the ability to support issue and action creation and tracking and ability to enter self-identified issues.	**3**	
b	The System should provide the ability to rate findings and issues.	**3**	
c	The System should provide the ability to link issues to one or more objectives, processes, risks, controls, action owners, oversight functions/reporting streams, etc.	**3**	
4.3.5	**Risk Reporting, KPIs and KRIs** The Proponent must respond by describing the System's risk reporting capabilities referencing the following:		
a	The System should provide the ability to create key risk indicators (KRIs) and track metrics, including at least: • Ability to link assessments to KRIs. • Ability to link KRIs to risk types or categories or controls. • Ability to link KRIs to loss events.	**3**	

	• Ability to trigger assessments of KRI thresholds being exceeded. • Ability to calculate metrics and KPIs (with the ability to set risk appetite and thresholds, graphically show when they are surpassed, and roll-up capabilities for calculated residual risk ratings for KRIs).		
b	The System should provide the ability to view information (risk, finding, issue, status of assessments, scores, weights, etc.) by line of business or on a consolidated basis (supporting multiple groupings, count, sum, etc.).	**3**	
c	The System should provide the ability to produce reports at any level of business hierarchy and span multiple levels of a business hierarchy or span multiple hierarchies.	**3**	
d	The System should provide the ability to set thresholds on specific numeric fields, display them graphically with conditional formatting, and send notifications based on exceeded thresholds.	**3**	
e	The System should provide the ability to maintain different threshold based on different associated business or asset hierarchy associations.	**3**	
f	The System should provide the ability to tier, aggregate or sum thresholds by multiple business lines or by event types.	**3**	
g	The System should provide the ability to generate on-line real time dashboards, trend analysis reports, largest risk reports, largest loss reports, assessment summary report, action plans report by multiple hierarchies.	**3**	
4.3.6	**Risk Acceptance** The Proponent must respond by describing the System's risk acceptance capabilities referencing the following:		
a	The System should provide the ability to have integrated findings/issues management feed into risk treatment and risk acceptance.	**3**	
b	The System should provide the ability to link risk acceptance to risk profiling, assessments, policies, compliance, and findings/issues management and the ability to adjust the profile score based on the number or amount of risk accepted by target profile.	**3**	
4.3.7	**Scenario Analysis** The Proponent must respond by describing the System's scenario analysis capabilities referencing the following:		

a	The System should provide the ability to perform scenario analysis, including at least: • Ability to baseline scenarios and re-validate on periodic basis and report against the results. • Ability to quantify scenarios and provide a hybrid capability for quant/qual analysis and risk calculations. • Ability to incorporate loss event data and history to create a holistic view of scenarios across the enterprise. Ability to apply scenarios across multiple entities and assets either individually or in any combination. Ability to store point-in-time scenario templates/forms that can be used for as necessary risk analysis.	**3**	
4.3.8	**Assessment Reporting** The Proponent must respond by describing the System's assessment reporting capabilities referencing the following:		
a	The System should provide the ability to aggregate risk Assessment results in terms of a heat map by any hierarchy (objectives, business, process, asset, risk, etc.) for reporting at any level and the ability to consolidate risk Assessment results by common data (risks) across any associated hierarchy.	**3**	
4.3.9	**Loss & Risk Event Capture** The Proponent must respond by describing the System's loss and risk event capture capabilities referencing the following:		
a	The System should provide the ability to manually input loss event data (create new or edit existing records).	**3**	
b	The System should provide the ability to automatically input loss event data (create new or edit existing records).	**3**	
c	The System should provide the ability to document root cause and impact analysis of loss events or near misses.	**3**	
d	The System should provide e-mail notifications and alerting to determined users when new loss events and near misses are captured for analysis.	**3**	
e	The System should provide the ability to support multiple types of loss events/categories and types of events that are recorded (i.e., pure losses, near misses, incidents, reputational events, etc.).	**3**	

f	The System should provide the ability to map types of loss events/categories to risk types, BASEL loss event categories and KRIs.	**3**	
g	The System should provide flexibility in allocation of loss (association) to one or multiple entities with the capability for loss event amounts to be aggregated or broken out individually over time.	**3**	
h	The System should provide the ability to adjust loss amounts based on recoveries either via manual entry or via calculation.	**3**	
4.4	**Internal Audit** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's internal audit requirements.	**15%**	
4.4.1	**Audit General Requirements** The Proponent must respond by describing the System's general audit requirement capabilities referencing the following:		
a	**Cross-Functional View** The system should provide the ability to allow users of the Internal Audit module to view (read-only) information from other modules to support planning of an audit (e.g., ERM risk assessments, RCSA's, issue resolution/ management actions outstanding, workplans of other oversight, etc.).	**3**	
b	**Process-Risk-Control Library** The system should provide the ability to document and maintain an organization-wide standardized process-risk-control library to which audit functionality would be linked to (e.g., Risk-Based Audit Plan (RBAP), issue resolution/ management actions listing, Assurance Map, etc.).	**3**	
c	**Required Fields** The system should provide the ability to indicate mandatory and optional fields for each type of record.	**2**	
d	**Access Management** The system should provide the ability to allow multiple users to edit records (e.g., objectives/criteria, controls, procedures, etc.) without overwriting changes from other users, to save previous versions, and to track updates.	**3**	
e	**Workflow Management** The system should provide the ability to do batch reviews and multiple-level reviews.	**2**	

f	**Library** The system should provide the ability to maintain and store templates/contents/procedures, etc. which can be used across projects or RBAP.	**3**	
g	**Record Retention** The system should provide the ability to retain information/files/working papers related to projects and RBAP for a minimum of 10 years.	**3**	
4.4.2	**Audit Plan** The Proponent must respond by describing the System's audit plan capabilities referencing the following:		
a	**Audit Universe/ Auditable Entities** The system should provide the ability to document and maintain hierarchies or structures within CMHC to which the Risk-Based Audit Plan (RBAP) and projects will be linked to.	**3**	
b	**Audit Plan** The system should provide the ability to document the periodic RBAP assessment and rating/scoring to identify projects to be included on plan, the ability to report on the status of the work plan, and the ability to link a project to its related RBAP assessment.	**3**	
4.4.3	**Conducting Projects** The Proponent must respond by describing the System's project capabilities referencing the following:		
a	**Project Profile** The system should provide the ability to document general information related to an audit client's business, objectives, risks, and controls, and the ability to add/configure fields (e.g., project metrics) associated with a project.	**3**	
b	**Risk Assessment** The system should provide the ability to add/ configure project inherent/residual risk rating/scoring to align with internal methodology.	**3**	
c	**Objectives, Controls and Procedures** The system should provide the ability to document project objectives/criteria, controls, and procedures (i.e., records), the ability to document and/or attach procedure step, guidance, templates, record of work done, conclusion, etc., and the ability to add/configure control	**3**	

	effectiveness field and project residual risk rating/scoring to align with Internal Audit methodology.		
d	**Project Closing** The system should provide the ability to prevent changes from being made after final audit report is issued, the ability to re-open closed projects if needed, and the ability to impose mandatory steps before project can be closed	**3**	
4.4.4	**Issue Management** The Proponent must respond by describing the System's issue management capabilities referencing the following:		
a	**Issues and Recommendation** The system should provide the ability to document project issues/observations and recommendations, including ownership, due dates, associated risks, type, etc., with the ability to tag configurable fields (e.g., assigning themes) to issues, the ability to develop action plans connected to observations and recommendations, and the ability to add/ configure priority rating/ scoring to align with Internal Audit methodology.	**3**	
b	**Issue Management** The system should provide the ability to track progress of released issue resolution/ management actions until remediated or accepted even after a project is closed, the ability to document updates related to issue resolution/ management actions (e.g., status updates, remediations, cancellations, etc.), and the ability to document issue resolution/ management actions validation procedures.	**3**	
4.4.5	**Budgeting, Resourcing and Scheduling** The Proponent must respond by describing the System's budgeting, resourcing, and scheduling capabilities referencing the following:		
a	**Capacity/Resource Planning at the RBAP level** The system should provide the ability to estimate start and end dates and assign resources (not individual users) to projects included in the Audit Plan. This is to ensure there are enough resources to complete the projects for the plan period.	**3**	
b	**Scheduling/Project Management at the RBAP level** The system should provide the ability to assign individual users and/or groups to projects included in the Audit Plan, and the ability to document planned start and end dates/ hours, actual start, and end dates/ hours,	**3**	

	and track the progress of the different milestone under each phase of the project.		
c	**Time Tracking/Timesheets** The system should provide the ability for each user (including consultant) to enter and track time spend and costs on projects by audit phase, resource type, etc. It should have the ability to aggregate the results by project/RBAP for comparison against budget.	**3**	
4.5	**Risk Appetite, Own Risk and Solvency Assessment (ORSA) and Enterprise Risk Management (ERM)** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's Risk Appetite, ORSA, and ERM requirements.	**3%**	
4.5.1	**Tracking Risk appetite** The Proponent must respond by describing the System's risk tracking appetite capabilities referencing the following:		
a	The system should have capabilities to support ERM and Risk appetite, including at least: • Ability to create multiple and detailed risk-specific statements on the goals, appetite, and tolerance levels for various risks, such as underwriting, credit, capital, liquidity, and operational risks. • Ability to measure/ evaluate risk metrics performance against risk appetite and tolerances. • Ability to generate dashboard demonstrating which measures associated with each appetite topic are near or outside of their tolerance (at least 20). • Ability to support / record results from stress testing and scenarios. • Ability to create and maintain a library of statutory, operational and market risks, potential risk events and scenarios that might cause an outflow of capital. • Ability to conduct or store results of Forward-looking Scenario Analysis forecasting and allocation with a forward-looking approach to solvency assessment under normal and severe stress scenarios.	**3**	

	• Ability to perform projected capital simulations or store results and supports capital calculation as ORSA guidelines.		
4.6	**Compliance** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's Compliance requirements.	**15%**	
4.6.1	**Regulations (data)** The Proponent must respond by describing the System's data regulations management capabilities referencing the following:		
a	The System should be able to house all regulations, executive orders, proposed rules, and guidance applicable to CMHC and its subsidiaries.	**3**	
b	System should have prepopulated regulations and frameworks (NIST, ISO, etc.).	**2**	
c	The System should be able to provide the past versions of the regulations.	**2**	
d	The System should allow users to assign an owner or group of users to each regulatory objective.	**3**	
e	The System should allow the ability to link the risk rating to the regulatory objective to allow the user to prioritize risks.	**3**	
f	The System should allow the capability to flag certain regulations as for information only but not critical to CMHC. It should allow for tagging of "critical" versus "information only".	**2**	
g	The System should provide the capability to risk assess the various regulations using a defined methodology (e.g., likelihood and impact factors).	**3**	
4.6.2	**Compliance Testing/Assessments** The Proponent must respond by describing the System's compliance risk assessment capabilities referencing the following:		
a	The System should provide the ability to perform high level and detailed compliance risk assessments (either via self assessment or facilitated assessments).	**3**	
4.6.3	**Compliance Reporting/KRIs** The Proponent must respond by describing the System's compliance reporting capabilities referencing the following:		

a	The System should be able to report on where regulations are in the review process at an aggregated level.	**3**	
b	The System should provide compliance dashboard reporting that various by department and management level.	**3**	
4.6.4	**Policy Management** The Proponent must respond by describing the System's policy management capabilities referencing the following:		
a	The System should be able to store corporate risk policies information and requirements and allow the creation of new policies.	**3**	
b	The System should provide version control for policies.	**3**	
c	The System should provide display status of a given policy (e.g., draft, in review, approved, etc.).	**3**	
d	The System should allow the user to generate a change summary of a policy that has been edited from a prior version.	**3**	
e	Policy approvers should have the option to approve or reject a policy with comments.	**3**	
f	The System should allow for multiple levels of approval.	**3**	
g	The System should allow the user to specify the timeline for policy review notifications, reminders, and past due alerts.	**3**	
h	The System should have functionality to retire policies that are no longer applicable.	**3**	
i	The System should allow a linkage to be created to related policies.	**3**	
j	The System should allow the ability to flag policies with proprietary information that need to be restricted.	**3**	
k	The System should allow policy exceptions to be tracked and monitored.	**3**	
4.6.5	**Privacy Operations** The Proponent must respond by describing the System's operational privacy capabilities referencing the following:		

a	The System should be able to store the information in our Personal Information Bank (PIB). For each line item on the PIB, the System should be able to maintain an association to the PIA (link) and map the vendor(s) involved (from vendor hierarchy).	**2**	
4.7	**Internal Controls** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's internal control requirements.	**10%**	
4.7.1	**Control Mapping and Scoping** The Proponent must respond by describing the System's control mapping and scoping capabilities referencing the following:		
a	Comprehensive control library to simplify the process of control identification and assessment.	**3**	
b	The System should provide the ability to maintain a standardized process-risk-control library associated with financial assertions.	**2**	
c	The System should support the Financial Statements Decomposition process (quantitative and qualitative) and tag related accounts.	**2**	
d	The System should support materiality calculations.	**2**	
e	The System should support linkages of Financial Statements Notes to processes.	**2**	
f	The System should provide the ability to maintain a standardized financial accounts-risk-control library.	**2**	
g	The System should provide the ability to easily track the key attributes of controls.	**3**	
h	The System should provide the ability to perform a gap analysis for risk, key control, and assertion coverage across lines of business.	**3**	
i	The System should provide the ability to create control review documentation including but not limited to Risk and Control Matrix, deficiency logs and briefing reports.	**3**	
4.7.2	**Control Testing/Assessments** The Proponent must respond by describing the System's control assessment capabilities referencing the following:		

a	The System should provide the ability to maintain high level and detailed control risk objectives.	**3**	
b	Should have ability to assess control design AND control operating effectiveness.	**3**	
c	The System should have the ability to have VARIOUS types of CONTROL classification, such as: 1. per type (manual, Manual IT Dependent, ITGC, etc.), 2. as preventative or detective controls, etc.	**3**	
d	The System should allow the user to perform ad-hoc monitoring/testing.	**3**	
e	The System should have the ability to add ad-hoc notes.	**3**	
4.7.3	**Control Deficiency Remediation** The Proponent must respond by describing the System's control deficiency remediation capabilities referencing the following:		
a	The System should provide the ability to document deficiencies and track them throughout their lifecycle (open, pending validation, validation procedures completed, closed).	**3**	
b	The System should provide the ability to classify deficiencies and maintain related documentation regarding the rationale for the categorization.	**3**	
4.7.4	**Control Monitoring and Reporting** The Proponent must respond by describing the System's control monitoring and reporting capabilities referencing the following:		
a	The System should be able to list compensating controls for key controls with deficiencies.	**2**	
b	The System should provide the ability to pull control information from assessments outside of the Internal Control module (e.g., Audit, Risk and Control Self-Assessment, Vendor Risk Assessment, IT Application Risk Assessment, etc.).	**3**	
c	The System should be able to aggregate controls by control performer, owner, and sector head.	**3**	
4.7.5	**SOX Attestation** The Proponent must respond by describing the System's SOX attestation capabilities referencing the following:		

a	The System should provide the ability to certify compliance with the International Financial Reporting Standards (IFRS) rules for internal control effectiveness over the organization's financial statements and be integrated with the current quarterly process.	**3**	
b	The System should provide the ability for process owners to attest to their processes.	**3**	
4.8	**Vendor Risk Management** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's vendor risk management requirements.	**3%**	
4.8.1	**Vendor Risk Management Requirements** The Proponent must respond by describing the System's vendor risk management capabilities referencing the following:		
a	The system should have a vendor risk module or capabilities, including at least: • The ability to capture supplier/vendor information and link them to other objects in the system (e.g., Organizational Hierarchy, Business Process, risks, systems controls, etc.). • Capture risk at the control and vendor levels. • Conduct periodic vendor risk assessments. • Risk assessment should support sending attestations to be completed by the vendors via system. • The system should have the ability for vendors to notify and provide information on incidents that impact the services provided. Including: incident description, dates and times, impacts, root cause analysis, remediation, etc. The system should have the ability to keep track of vendor related information, such as: contingency and exit strategies, BCP and DR testing results and SOC reports and vendor attestations.	**3**	
4.9	**IT Risk and Security** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's IT risk and security requirements.	**3%**	

4.9.1	**IT Risk General requirements** The Proponent must respond by describing the System's IT risk capabilities referencing the following:		
a	The system should have a vendor risk module or capabilities, including at least: • Out of the box technology vendor products that can be used as a reference for assets, drop down lists, etc. and be able to connect or leverage data in ServiceNow and ability to classify assets under various parameters (e.g., financially significant, application criticality tier). • Should be able to reuse the application inventory details with other GRC modules in the system (e.g., Vendor Management, Audit Management, etc.). • Ability to profile IT risks. • Ability to perform TRAs and privacy risk assessments. • Should be able to interface with existing external Threat & Vulnerability intelligence services such as the Canadian Centre for Cyber Security. • Should have the ability to import data from various information security tools (e.g., scanners, Qualys, MS sentinel and Defender, etc.). • Ability to analyze the results of threat and vulnerability data to identify/prioritize vulnerabilities and create watch lists. • Should have the ability to store information on the latest patches released by software vendors that mitigate specific vulnerabilities and link to associated vulnerabilities. • The system should have the ability to tie scanning data to enterprise assets.	**3**	
4.10	**Business Continuity Management (BCM) and Disaster Recovery Planning (DRP)** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's BCM and DRP requirements.	**3%**	

4.10.1	**BCM and DRP Requirements** The Proponent must respond by describing the System's BCN and DRP capabilities referencing the following:		
a	The system should have a Business Continuity Management (BCM) module or capabilities, including at least: • Ability to store a library of BCP and DR Plans and5 years of audit trail of changes. • Ability to manage/ store results of BCM/DR assessments/ exercise. • Track completion, target, and overdue dates. • Allow for creation of a business/disaster recovery plan and its components, testing components and details. • Ability to manage CMHC's business impact analysis (BIA) including recording of results and managing findings/issues. • Ability to track and report on lessons learned post incidents and action plans resulting from these.	**3**	
4.11	**Model Risk Management** The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's model risk management requirements.	**3%**	
4.11.1	**Model Inventory and Risk Assessment** The Proponent must respond by describing the System's model inventory and risk assessment capabilities referencing the following:		
a	The system should have a model risk module or capabilities, including at least: • Ability to create an inventory of Models. • Ability to track and manage the Model Lifecycle Management (e.g., User requirement gathering, In Development or procurement, Development status, Validation status (draft and final), Approved for Use, Active, Ongoing Monitoring, Retired, etc.). • Ability to generate or associate model risk assessments with loss event records, KRIs and issues.	**3**	
4.12	**Environmental, Social, and Governance (ESG) Management**	**3%**	

	The proponent must provide detailed information relative to each of the functional requirements set out below demonstrating their proposed System meets CMHC's ESG management requirements.		
4.12.1	**ESG Risk Assessment** The Proponent must respond by describing the System's ESG risk assessment capabilities referencing the following:		
a	The system should have an ESG risk module or related capabilities, including at least: • Ability to create and track an inventory of ESG metrics and related data (*including, among others, metrics used for climate risk management-assessment, target setting, reporting, and performance improvement). • Ability to perform ESG materiality assessment. • Ability to track Climate impacts to other risks and when climate is a driver of other risk types/events. • Ability to link ESG risks to goals, appetite and tolerance levels for various risks, business units, processes, controls, etc. • Ability to configure an ESG risk assessments and surveys and to use "assessment" functionality on a broader basis for information gathering.	**3**	

APPENDIX D – FORM OF AGREEMENT

CMHC SOFTWARE-AS-A-SERVICE ("SaaS") AGREEMENT

CMHC FILE No. PA# _____

THIS SaaS AGREEMENT ("Agreement") is executed

BETWEEN:

CANADA MORTGAGE AND HOUSING CORPORATION
700 Montreal Road
Ottawa, Ontario, K1A 0P7

(Hereinafter referred to as "**CMHC**")

- and -

FULL LEGAL NAME OF THE SELECTED PROPONENT
Address of the selected proponent

(Hereinafter referred to as the "**Contractor**")
(Each individually a "**Party**" and collectively the "**Parties**")

ARTICLE I. DEFINITIONS

"Authorized User" means any individual or entity authorized by CMHC to access and use the SaaS Services through CMHC's account under this Agreement, each of which shall be identified by CMHC's written notice to the Contractor as set forth in Schedule A (the "SaaS Services") of this Agreement.

"**CMHC Content**" means any content, materials, data and information that CMHC, its Authorized Users, or authorized Contractor personnel or subcontractors, may enter into the SaaS Services or is otherwise uploaded by or on behalf of CMHC. For clarity, CMHC Content will not include any component of the SaaS Services or Contractor's Intellectual Property.

"CMHC Information" refers to any and all information of a confidential nature that is transferred, directly or indirectly, to the Contractor or for which access is provided to the Contractor including all Personal Information, that is in the care or control of CMHC, and is managed, accessed, collected, used, disclosed, retained, received, created or disposed of in relation to the provision of the SaaS Services, including CMHC Content, whether or not it is marked as confidential. Without limiting the generality of the foregoing, CMHC Information includes data in any format, whether or not marked as confidential.

"Confidential Information" means "collectively the following categories of information: (i) the terms of this Agreement (except to the extent that the disclosure of this Agreement or parts thereof is permitted or required pursuant to applicable Laws);

(ii) all proprietary business, financial, and technical information of the disclosing Party that is disclosed under circumstances reasonably implying that such information should be treated confidentially, including without limitation CMHC lists and associated CMHC information, know-how, methods, processes, analyses, framework, strategies, marketing plans, designs, specifications, development plans, business plans, prices, sales projections, and trade secrets of the other Party; (iii) any employee-related information or similar information provided by one Party to the other Party; (iv) for the purposes of CMHC, CMHC Content and CMHC Information; and (v) the SaaS Services and Documentation.

"Documentation" means all generally available documentation relating to the SaaS Services, including all user manuals, operating manuals and other instructions, specifications, documents and materials, in any form or media, that describe any component, feature, requirement or other aspect of the SaaS Services, including any functionality, testing, operation, or use thereof.

"Harmful Code" means any software, hardware or other technologies, devices, or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner, any (i) computer, software, firmware, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use, or operation of any data processed thereby; or (b) prevent CMHC or any Authorized User from accessing or using the SaaS Services as intended by this Agreement, and includes any virus, bug, Trojan horse, worm, backdoor, malware or other malicious computer code, and any time bomb or drop-dead device.

"**Intellectual Property Rights**" means unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, mask work rights, know-how and other trade secret rights, and all other intellectual property rights, derivatives thereof, and forms of protection of a similar nature.

"Laws" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement of any federal, provincial, territorial, municipal or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction.

"Losses" means any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, fees and the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers.

"Personal Information" means information about an identifiable individual or other information that is subject to Canadian privacy Laws.

"SaaS Services" means a hosted solution made available by the Contractor for CMHC's access and use on a subscription basis, as detailed in Schedule A (the "SaaS Services"). The term "SaaS Services" includes any modifications, enhancements, additions, extensions, translations, and derivative works thereof and any configuration and related services. The SaaS Services do not include CMHC Information or any CMHC-provided third party software.

ARTICLE II. SAAS SERVICES

SECTION 2.01 DESCRIPTION OF SAAS SERVICES

(a) This Agreement sets out the general terms and conditions for the provision of the SaaS Services by the Contractor to CMHC, as further defined in Schedule A (the "SaaS Services") of this Agreement.

(b) The capitalized terms as used in this Agreement have the meanings set out in the body of this Agreement or Article I Definitions.

ARTICLE III. REPRESENTATIONS AND WARRANTIES

SECTION 3.01 THE CONTRACTOR REPRESENTS AND WARRANTS THAT:

(c) It is validly incorporated (or formed), it continues to be in valid existence and, if applicable, good standing in the jurisdiction of its incorporation or formation;

(d) It has obtained, and will maintain at all times during the term of this Agreement, all necessary registrations, licenses and consents and comply with all relevant Laws applicable to the provision of the SaaS Services;

(e) The execution of this Agreement by its representative whose signature is set forth at the end hereof has been duly authorized by all necessary corporate action of the Contractor;

(f) It shall comply with all applicable rules, regulations, and policies of CMHC, including security procedures concerning systems and data and remote access thereto, building security procedures, including the restriction of access by CMHC to certain areas of its premises or systems for security reasons, and general health and safety practices and procedures;

(g) The Contractor warrants that the SaaS Services provided to CMHC pursuant to this Agreement will comply in all material respects with the terms of this Agreement;

(h) the SaaS Services are and will remain free of Harmful Code;

(i) It shall provide the SaaS Services using personnel of required skill, experience, and qualifications;

(j) It shall provide the SaaS Services in a timely, workmanlike and professional manner and in accordance with the applicable industry standards in the Contractor's field; and

(k) It shall ensure that all of its equipment and/or software used in the provision of the SaaS Services is in good working order and suitable for the purposes for which it is used.

The warranties set forth in this Section are cumulative and in addition to any other warranty provided by law or equity.

ARTICLE IV. TERM AND TERMINATION

SECTION 4.01 TERM

The term of the Agreement shall be for an initial period of three (3) years commencing on _____, 2024 (the “Effective Date”) and ending on _____, 2027 (the “Initial Term”).

SECTION 4.02 RENEWAL

This Agreement may be extended, at the option of CMHC, for up to two (2) additional one (1) year terms (the “Extension Term”), not to exceed a cumulative five (5) years including the Initial Term. The Initial Term and any Extension Term herewith collectively referred to as the “**Term**”.

SECTION 4.03 TERMINATION

(A) **NO FAULT TERMINATION**

Notwithstanding 0 and 0 above, CMHC may terminate the Agreement for any reason with no penalty or charge by giving Choose an item days prior written notice at any time during the Term.

(B) **TERMINATION FOR DEFAULT OF THE CONTRACTOR**

CMHC may terminate this Agreement without penalty or charge, and, with or without notice, as applicable, for the following reasons:

The Contractor commits a material breach of its duties under this Agreement, numerous breaches of its duties under this Agreement that collectively constitute a material breach, unless the Contractor cures such breach and indemnifies CMHC for any resulting damage or loss, both in a manner satisfactory to CMHC in its sole, absolute and non-reviewable discretion, within twenty (20) calendar days of receipt of written notice of breach from CMHC; Without notice if there is a change in control of the Contractor where such control is acquired, directly or indirectly, in a single transaction or series of related transactions, or all or substantially all of the assets of the Contractor are acquired by any entity, or the Contractor is merged with or into another entity to form a new entity, unless the Contractor demonstrates to the satisfaction of CMHC that such event will not adversely affect its ability to perform the SaaS Services under this Agreement; or Without notice if the Contractor becomes bankrupt or insolvent, or a receiving order is made against the Contractor, or any assignment is made for the benefit of the creditors, or if an order is made or a resolution passed for the winding up of the Contractor.

Without notice if CMHC has reason to believe that the Contractor has committed gross misconduct, fraud or other unlawful acts, a breach of its Representation and Warrantees under Article III, or a breach of its obligations with regard to Article VII (Confidentiality and Privacy), or 0 (article viii. Intellectual Property).

SECTION 4.04 CMHC'S OBLIGATIONS UPON TERMINATION

In the event that a notice of termination is given, and subject to the deduction of any claim which CMHC may have against the Contractor arising out of the Agreement or its termination, CMHC will make payment for the value of all SaaS Services performed to the date of the notice, as determined in accordance with the rate(s) specified in Schedule B (the "Fees") of this Agreement. CMHC shall make payment within thirty (30) days as of (i) the date of the notice; or (ii) receipt of an invoice submitted by the Contractor, whichever is later. Upon such payment, it shall have no further obligation or liability of any kind to the Contractor.

SECTION 4.05 CONTRACTOR'S OBLIGATIONS UPON TERMINATION

Upon the effective date of expiration or termination of this Agreement:

(a) The Contractor shall, at CMHC's option and upon its written request return or destroy CMHC Information in the manner set forth in Article VII and Schedule C (the "Privacy and Security Requirements") of this Agreement;

(b) at CMHC's option and upon its written request, the Contractor shall: (1) continue to retain the CMHC Information, or solely such specific databases or other collections or articles of CMHC Information as CMHC may request, as though this Agreement were still in force, for a period to be agreed to by the Parties in writing, but that in no event will be shorter than forty five (45) calendar days or longer than one hundred and eighty (180) calendar days after the effective date of such expiration or termination, as applicable, provided that CMHC pays in full all undisputed fees due to the Contractor as of the effective date of such expiration or termination and pays monthly data storage fees to the Contractor for its retention of such CMHC Information at no additional cost to CMHC; and (2) immediately upon the conclusion of such CMHC Information retention period, return such CMHC Information by taking all steps required or reasonably requested to assist CMHC in migrating such CMHC Information to CMHC systems in both the Contractor's data format and a platform-agnostic format.

(c) If, exercising its rights under Section 4.03 (a) or Section 4.03 (b), CMHC elects to terminate this Agreement, the Contractor shall refund to CMHC all fees paid to the Contractor for SaaS Services that were not provided under this Agreement. All refunds payable under this 0(c) shall be paid within thirty (30) days of CMHC's written notice of termination.

ARTICLE V. PRICE AND PAYMENT

SECTION 5.01 PRICING

Subject to the terms and conditions of this Agreement, CMHC shall pay the fees set forth in Schedule B (the "Fees") of this Agreement plus applicable taxes. Notwithstanding any other provision in this Agreement, CMHC's total financial obligation for the SaaS Services provided under the Agreement shall not exceed $_____ dollars CAD inclusive of taxes, assessment, duties, levies and expenses during the Term of the Agreement. No other taxes, assessments, duties or other levies shall be payable to the Contractor unless specifically agreed to in writing by the Contractor and CMHC.

SECTION 5.02 INVOICING

(d) The Contractor shall submit, where applicable, detailed invoices to CMHC during the Term. The Contractor must allow thirty (30) days from delivery of invoice for payment without interest charges. The Contractor cannot invoice prior to performance of the SaaS Service. CMHC may, if applicable, issue an annual Purchase Order (PO) Number for invoices to be processed in the applicable year under this Agreement.

All invoices of the applicable year must make reference to the corresponding PO number and shall be sent electronically to _____@cmhc-schl.gc.ca with a copy to accountspayable@cmhc-schl.gc.ca

(e) GST/HST or Provincial sales taxes, as applicable, shall be collected by the Contractor and shown as a separate item on each invoice, showing the Contractor's GST/HST/ QST or other provincial tax numbers, as applicable. The Contractor shall duly remit to the Canada Revenue Agency or the appropriate provincial taxing authorities all taxes payable on the SaaS Services.

SECTION 5.03 VERIFICATION OF PERFORMANCE

Before advancing any amount to the Contractor, CMHC reserves the right to determine, whether the SaaS Services were performed in accordance with the terms and conditions of this Agreement. In the event that the SaaS Services do not meet the standards set out in this Agreement, CMHC may take such action as reasonably necessary to require the Contractor to correct its default, including, without limitation, the following:

(f) requiring the Contractor to refund the portion of fees related to the SaaS Services that do not meet the standards set out in this Agreement;

(g) withholding payment;

(h) setting off any expenses incurred by CMHC in remedying the default of the Contractor against payment for payment due to the Contractor; and/ or

(i) terminating the Agreement for default.

SECTION 5.04 WITHHOLDING TAXES

NOTE: This clause is applicable to foreign contractors for services rendered in Canada.

Any payments made to the Contractor by CMHC pursuant to Article 5 in respect of services rendered in Canada will be subject to a fifteen percent (15%) withholding tax as required pursuant to Regulation

105 of the Income Tax Act. If any such withholding taxes are required to be withheld from any amounts payable to the Contractor, CMHC shall make such withholdings and duly and promptly remit the amount withheld to the Canada Revenue Agency. The Contractor must identify the value of services provided in Canada within its invoice. Otherwise, CMHC will withhold taxes on the full consideration amount.

CMHC shall have no liability or responsibility for withholding or remitting any taxes or payments, including but not limited to employment insurance remittances, Canada Pension Plan contributions or employer health tax, or worker's compensation insurance premiums for Contractor and Contractor Personnel. The Contractor is responsible for these withholding, remitting and registration obligations, and shall indemnify CMHC from and against any order, penalty, interest, taxes or contributions that may be assessed against CMHC due to the failure or delay of Contactor to make any such withholdings, remittances or registration, or to file any information required by any law.

SECTION 5.05 METHOD OF PAYMENT

All payments due under the Agreement will be made by means of Electronic Funds Transfer ("EFT"). The Contractor shall provide CMHC with all information set out in 0 to allow EFT to be effected and keeping the information up to date. In the event that CMHC or the Contractor is unable to make/accept payment by EFT, the Contractor agrees to accept payment by cheque or another mutually agreeable method of payment.

SECTION 5.06 TIMING OF PAYMENT

The Contractor shall allow CMHC thirty (30) days from delivery of invoice for payment without interest charges, except for any amounts disputed by CMHC in good faith.

SECTION 5.07 DISBURSEMENTS AND TRAVEL COSTS

The Contractor is not entitled to seek reimbursement from CMHC for any extra or separate travel expenses whatsoever under this Agreement that have not been pre-approved and authorized

SECTION 5.08 DIRECT DEPOSIT AND INCOME TAX REPORTING REQUIREMENT

Under the Income Tax Act, CMHC must report payments to contractors to the Government of Canada by issuing a T1204 supplementary slip. The Contractor shall provide CMHC the necessary information to complete any forms to comply with its obligation under the Income Tax Act or any law, including the Contractor's business number, in order to allow CMHC to make payment by EFT and to complete the T1204 supplementary slip. In the event that the Contractor is an individual and does not have a Business Number issued by the CRA, the Contractor must provide their Social Insurance Number.

The Contractor shall complete the Vendor Information Form under Schedule B (the "Fees") prior to commencement of the Term. Throughout the Term, the Contractor shall ensure that the information provided remains accurate and up to date. The Contractor assumes full responsibility for any errors in payments or tax reporting that arise because the information supplied is inaccurate or out of date. In addition, the Contractor shall provide contact information to CMHC to allow for payment by EFT including a void cheque.

SECTION 5.09 PAYMENT DISPUTE

In the event of a payment dispute, CMHC shall deliver a written statement to the Contractor listing all disputed items and providing an explanation of each disputed item.

Amounts not so disputed are deemed accepted and must be paid, notwithstanding disputes on other items, within the period set forth in this Section. The Parties shall seek to resolve all such disputes

expeditiously and in good faith. Contractor shall continue performing its obligations under this Agreement notwithstanding any such dispute.

SECTION 5.10 REMEDIES FOR NON-COMPLIANCE

If the Contractor fails to comply with a direction or decision of CMHC properly given under the terms of the Agreement, CMHC may take such actions and incur such costs that are reasonably required to implement its direction including, without limitation, the engagement of another person or entity to perform the SaaS Service and withholding of payment due to the Contractor for SaaS Services rendered, which moneys may be set off by CMHC against any expenses that it may incur in remedying a default or failures as described above.

ARTICLE VI. CONFLICT OF INTEREST

SECTION 6.01 NO BRIBE OR CONFLICT OF INTEREST

The Contractor and its principals, employees, agents and subcontractors declare that no bribe, gift, benefit, or other inducement has been or will be received or paid, given, promised or offered directly or indirectly to any official or employee of CMHC and shall declare any real, potential or apparent conflict of interest to CMHC immediately upon becoming aware of the conflict. The Contractor must not influence, seek to influence or otherwise take part in a decision of or about CMHC knowing that the decision might further its private interest. Conflict of interest means any matter, circumstance, interest, or activity affecting the Contractor, its personnel or subcontractors, which may or may appear to impair the ability of the Contractor to perform the work under this Agreement diligently and independently.

SECTION 6.02 THIRD PARTY CONFLICTS OF INTERESTS

The Contractor must have no financial interest in the business of a third party that causes or appears to cause a conflict of interest in connection with the performance of its obligations under the Agreement. If such an interest is acquired during the Term of the Agreement, the Contractor must immediately declare it to CMHC.

SECTION 6.03 WARRANTY OF DILIGENT INQUIRY

The Contractor warrants that, to the best of its knowledge after making diligent inquiry, no conflict exists or is likely to arise in the performance of the Agreement. In the event the Contractor becomes aware of any matter that causes or is likely to cause a conflict of interest in relation to the Contractor's performance under the Agreement, the Contractor must immediately disclose such matter to CMHC in writing.

SECTION 6.04 TERMINATION FOR CONFLICT OF INTEREST

In the event that a conflict of interest, real, potential or perceived, cannot be resolved to the satisfaction of CMHC, CMHC shall have the right to immediately terminate the Agreement.

SECTION 6.05 TRANSFER OF WORK PRODUCT UPON TERMINATION

Intentionally Removed.

SECTION 6.06 COMPLIANCE WITH CONFLICT OF INTEREST ACT

Any public office holder or former public office holder must be in compliance with the provisions of the *Conflict of Interest Act* in order to derive a direct benefit from any Agreement which may arise from this request for proposal.

ARTICLE VII. CONFIDENTIALITY AND PRIVACY

SECTION 7.01 CONFIDENTIALITY AND NON-DISCLOSURE OF CMHC INFORMATION

(a) Each Party shall treat all Confidential Information of the other Party as proprietary, confidential and sensitive unless otherwise specifically agreed to in writing by both Parties. Both Parties shall restrict access to the other Party's Confidential Information to those persons who have a need to know this Confidential Information in order to perform such person's obligations under the Agreement provided such parties are bound by substantially similar obligations of confidentiality.

(b) Each Party shall, in its capacity as receiving party, use at least the same degree of care as it employs to protect its own Confidential Information of a similar nature, but in any event no less than a standard of care that is consistent with industry standards, to maintain the confidentiality of all Confidential Information of the disclosing party that it handles, including, in the case of the Contractor complying with any applicable security requirements described in Schedule C (the "Privacy and Security Requirements").

(c) The Contractor understands the sensitive nature of the CMHC Information and agrees to treat all CMHC Information as proprietary, confidential and sensitive during the Term and following termination of the Agreement, unless otherwise specifically agreed to in writing by CMHC.

(d) The Contractor further agrees to restrict access to CMHC Information to those persons who have a need to know this information in order to perform the SaaS Services and who are bound by an obligation of confidentiality that is as strict as that contained in this Agreement provided such persons meet the appropriate security screening as per Government of Canada security screening classification prior to CMHC granting any such access. Where the SaaS Services are sensitive in nature, CMHC may require that the Contractor provide an oath of secrecy for each of its employees or persons engaged in performing the SaaS Services.

(e) In the event that the Contractor experiences a breach of confidentiality with respect to CMHC Information, the Contractor will immediately notify CMHC and co-operate with CMHC to the extent required to remedy the breach.

(f) The Contractor further acknowledges and understands that CMHC considers all CMHC Information to be under its custody and control at all times, and that all information in the care and control of CMHC is subject to federal Laws on privacy and access to information.

(g) The Contractor shall, at all times, ensure to transmit information between the Contractor and CMHC through secure means of transmission.

(h) In addition, when CMHC Information is stored, the Contractor will, at all times, use reasonable administrative, physical and technological security measures to ensure that the information remains confidential where applicable, and that the information is not lost or otherwise accessed without authority, as further described in Schedule C attached hereto. The Contractor will also implement information management and governance tools and controls, as further described in Schedule C. The requirements of Schedule C will be binding on any third party to whom the Contractor outsources any of its information technology or information management functions or who is managing such functions on behalf of the Contractor. In addition to the requirements set forth in Schedule C, the Contractor shall, to the extent the information contains Personal Information, comply with applicable Canadian privacy Laws.

(i) The Contractor shall conduct regular security assessments to ensure safeguards are working effectively.

(j) The Contractor shall ensure all CMHC Information is encrypted while in transit and at rest at a minimum one hundred and twenty-eight (128) bit encryption throughout the Term.

(k) Any CMHC Information provided to the Contractor in the performance of the SaaS Services shall be returned, uncopied to CMHC or destroyed by the Contractor immediately following the termination of this Agreement or upon the request of CMHC. For documents not returned to CMHC, the Contractor shall proceed with the destruction of such documents in accordance with CMHC's reasonable instructions and provide specific proof under oath of their destruction. Notwithstanding the foregoing, the Contractor shall be permitted to maintain copies of such documentation as it reasonably required in accordance with records retention or other regulatory requirements, provided that such retained documentation shall at all times remain subject to the other provisions of this Agreement.

(l) The Contractor shall ensure that employees, sub-contractors and/or service providers who have a need to know to CMHC's Information are made aware of the confidentiality, data handling and security requirements set forth in this Agreement.

(m) Without limiting the generality of the foregoing, the Contractor shall not and shall ensure that any subcontractor, reseller, agent or any other entity engaged to perform any portion of the SaaS Services does not release, share or otherwise divulge CMHC Information to any other entity including subsidiaries, branch offices, partners of the Contractor or subcontractors without the prior written consent of CMHC.

(n) The Contractor may disclose CMHC Information where required to do so pursuant to a lawful requirement or for the purposes of complying with a subpoena, warrant or other legal compulsion lawfully made by a court or other competent authority. When the Contractor discovers that it may potentially be required to disclose CMHC Information for the reasons described in the immediately foregoing sentence, the Contractor shall: (1) notify CMHC promptly so that CMHC has the opportunity to seek a protective order or other appropriate remedy; (2) provide information and other assistance in order for CMHC to take appropriate legal action against disclosure; and (3) ensure that disclosure is strictly limited to the information lawfully requested.

(o) Employees of the Contractor may be required to undergo criminal records check or hold a valid personnel security screening at the level of Enhanced Reliability prior to commencement of any SaaS Services and must provide the results of the check to CMHC's corporate security department. CMHC reserves the right to disallow any person to carry out work under the Agreement on the basis of the results of the criminal records check/security clearance. Each of the Contractor's proposed staff, who do not hold a valid clearance, will be required to complete a "Security Clearance Form" (67934) upon request from CMHC

SECTION 7.02 PRIVACY

Contractor acknowledges and agrees that all Personal Information collected or accessible to Contractor in the course of providing the SaaS Services, including CMHC Personal Information constitutes Confidential Information of CMHC to which the provisions of 0 apply, except to the extent such provisions are inconsistent with this 0, which prevails with respect to CMHC Personal Information. In addition to the foregoing obligations, Contractor will:

(a) Handle all CMHC Personal Information in accordance with Canadian privacy Laws;

(b) Subject to 00, perform its obligations under this Agreement in a manner that will facilitate CMHC's compliance with Canadian privacy Laws;

(c) Comply with such privacy measures as further described in SCHEDULE "D" ("Privacy and Security Requirements"), attached hereto;

(d) if requested by CMHC, within five business days from the date upon which the request was made by CMHC, to the extent the Contractor has possession or control of CMHC Personal Information, either: (i) update, correct or delete CMHC Personal Information or modify the individual's choices with respect to the permitted use by CMHC of such CMHC Personal Information; or (ii) provide access to CMHC or to its other service providers to enable it to perform the activities described in clause (i) itself;

(e) if the Contractor receives a request for access to CMHC Personal Information that is under the possession or control of the Contractor immediately refer such request to CMHC, and respond to any such request only by making reference to such referral; and, if CMHC is required by any Canadian privacy Laws to provide CMHC Personal Information to an individual that is in the Contractor's possession or control, at CMHC's request, provide such CMHC Personal Information to CMHC on or before the deadlines for such provision required to enable CMHC to comply with any deadlines applicable under such Canadian privacy Laws to the provision of such CMHC Personal Information, provided that CMHC has given the Contractor sufficient notice to meet such deadlines;

(f) if not legally prohibited (or has received a request from a law enforcement official to refrain) from doing so, notify CMHC of any subpoena, warrant, order, demand, requirement or request (including any national security letter) made by a governmental or regulatory authority for the disclosure of CMHC Personal Information, and, to the maximum extent permitted by applicable Laws, reasonably cooperate with CMHC in its efforts to oppose, seek judicial relief of and appeal any such subpoena, warrant, order, demand, requirement or request;

(g) immediately notify CMHC if the Contractor receives notice from any governmental or regulatory authority alleging that CMHC or the Contractor has failed to comply with Canadian privacy Laws in connection with the performance of this Agreement, or if the Contractor otherwise becomes aware and reasonably believes that the Contractor or CMHC may have failed or may in the future fail to comply with Canadian privacy Laws in connection with the performance of this Agreement;

(h) at CMHC's direction, cooperate and comply with any requests or instructions issued by any privacy or data protection authority, including any governmental or regulatory authority applicable to CMHC or CMHC Personal Information;

(i) provide reasonable assistance to CMHC in responding to and addressing any complaint relating to the handling of CMHC Personal Information in the course of the performance of the SaaS Services; and

(j) upon CMHC's written request, provide CMHC with an updated list of all the Contractor personnel that have handled CMHC Personal Information. In addition to the attestations to be provided by the Contractor elsewhere in this Agreement, the Contractor agrees that within one and hundred eighty (180) days following the execution of this Agreement and, on an annual basis thereafter, it shall cause a duly authorized senior executive of the Contractor and of the Contractor's subcontractors, as applicable, to provide CMHC with a letter attesting that the Contractor and the Contractor's subcontractors have complied with the requirements of the Agreement.

SECTION 7.03 PRIVACY BREACH NOTIFICATION

Upon becoming aware of the occurrence of any potential or confirmed security breach or privacy breach, the Contractor will do the following, subject to applicable Laws.

(a) immediately, but in any event not later than two (2) business days from the date Contractor becomes aware of the occurrence of such security breach or privacy breach, notify CMHC by telephone and in writing;

(b) take all steps necessary to enforce against any person that is or may be engaging in such unauthorized handling any rights that the Contractor has to require such person to comply with any obligation of confidence to the Contractor and to cease such unauthorized activities;

(c) do all things, execute all documents and give all assistance reasonably required by CMHC to enable CMHC to enforce against any person that is or may be engaging in such unauthorized handling any rights that CMHC must require such person to comply with any obligation of confidence to CMHC and to cease such unauthorized activities; and

(d) if the security breach involves CMHC Personal Information, then, if requested by CMHC, reasonably cooperate with and assist CMHC in CMHC's communication with the media, any affected persons (by press release, telephone, letter, call centre, website, or any other method of communication) and any governmental or regulatory authorities to explain the occurrence of the security breach and the remedial efforts being undertaken. The content and method of any such communications will be determined by CMHC and the Contractor, to the extent such content refers to the Contractor, acting reasonably. Additionally, the Contractor shall assist CMHC in mitigating any potential damage and take such commercial steps as are directed by CMHC to assist in the investigation, mitigation and remediation of each such security breach. As soon as reasonably practicable after any such security breach, the Contractor shall conduct a root cause analysis and, upon request, will share the results of its analysis and its remediation plan with CMHC. The Contractor shall provide updated information to CMHC should additional details be discovered regarding the cause, nature, consequences, or extent of the security breach.

SECTION 7.04 ACCESS TO INFORMATION

The Contractor acknowledges that the Access to Information Act applies to CMHC and may require the disclosure of information. The Parties will comply with the provisions of the Access to Information Act, including in connection with a request under the Access to Information Act by a third party for access to information ("Access to Information Act Request").

If an Access to Information Act Request is made to the Contractor (rather than to CMHC) for access to any CMHC Information, the Contractor will: (a) not communicate with or respond to the person making the Access to Information Act Request, except as directed by CMHC in writing; (b) promptly, but in any event within seven days (or such other period of time as may be agreed by the Parties) of the receipt of such Access to Information Act Request, forward that Access to Information Act Request to CMHC; and (c) without detracting from CMHC's responsibilities and the Contractor's rights under the Access to Information Act, reasonably cooperate with CMHC as necessary to enable CMHC to respond to each Access to Information Act Request or otherwise comply with the Access to Information Act.

SECTION 7.05 DATA RESIDENCY AND DATA ACCESS

A. CMHC information to remain in Canada

(i) The Contractor agrees that the CMHC Information shall always remain in Canada and it shall not relocate the equipment, databases or documents containing any data (including any redundant or back-up environments) anywhere outside of Canada without CMHC's prior written consent.

(ii) The Contractor shall ensure that only employees, sub-contractors and/or service providers located in Canada, who have a need to know to CMHC's Information and who have obtained the appropriate security screening as per Government of Canada security screening classification, will have access to such CMHC Information. Supplier shall prevent and disable any access to CMHC's Information to employees, sub-contractors and/or service providers located outside of Canada.

(iii) Contractor agrees to logically segregate CMHC Information in electronic format and physically segregate physical documents.

B. Exception for Regular Business Communication

Keeping CMHC Information exclusively in Canada is not mandatory for regular business communication that does not include sensitive and/or protected or secret information or Personal Information. Notwithstanding the foregoing, both Parties agree that only CMHC Information (excluding CMHC Content) required for the management of the relationship between the Contractor and CMHC (for example, billing information, contact information for managing the contractual relationship, etc.) may be stored and processed outside of Canada.

SECTION 7.06 REVIEW OF AGREEMENT

CMHC may, from time to time, require a review of the privacy and security clauses set forth in the Agreement and Contractor shall collaborate with CMHC in such review, and, where appropriate, will agree to update such privacy and security clauses to ensure CMHC remains compliant with regulatory requirements or direction.

ARTICLE VIII. INTELLECTUAL PROPERTY

SECTION 8.01 LICENSE OF SAAS SERVICES

Subject to the terms and conditions of this Agreement, Contractor hereby grants to CMHC a non-exclusive, irrevocable right and license to permit its Authorized Users to access and use the SaaS Services.

SECTION 8.02 OWNERSHIP OF CMHC INFORMATION

CMHC may, but is not required to, provide CMHC Information to the Contractor in connection with this Agreement. CMHC is and will remain the sole and exclusive owner of all right, title, and interest in and to all CMHC Information, including all Intellectual Property Rights relating thereto, subject only to the limited licence granted in 0.

SECTION 8.03 LIMITED LICENCE TO USE CMHC INFORMATION

Subject to the terms and conditions of this Agreement, CMHC hereby grants the Contractor a limited, royalty-free, fully paid-up, non-exclusive, non-transferable non-sublicensable licence to process the CMHC Information in Canada strictly as instructed by CMHC or an Authorized User and solely as necessary to provide the SaaS Services for CMHC's benefit as provided in this Agreement.

SECTION 8.04 OWNERSHIP OF CONTRACTOR MATERIALS

The Contractor (and its licensors, where applicable) own all right, title and interest, including all Intellectual Property Rights, in and to the systems, software and other content and materials used in the provision of the SaaS Services.

SECTION 8.05 CORPORATE IDENTIFICATION AND BRANDING

It is agreed that the Contractor shall make no use whatsoever of CMHC's name, logo or other official marks without the express written consent of CMHC.

ARTICLE IX. AUDIT

The Contractor shall keep complete and accurate records and statements relating to this Agreement during the Term and for a period of seven (7) years following the end of the Term and any renewals thereof. Subject to reasonable prior notice, The Contractor shall permit inspection of such records and statements by CMHC's internal or external auditors.

The Contractor shall provide CMHC and/or its auditors with sufficient original documents in order to conduct the audit and allow CMHC to inspect and make copies of such records and interview the Contractor personnel in connection with the provision of the SaaS Services at its own expense. CMHC agrees to cooperate with the Contractor in the course of conducting any audit in order to avoid disruption in day-to-day operations.

ARTICLE X. CONTINGENCY PLANNING

SECTION 10.01 BUSINESS CONTINUITY PLANNING

The Contractor shall maintain its own business continuity plan, disaster recovery plan and procedures and will cause any affiliates or approved subcontractors performing in the delivery of services under this Agreement to likewise maintain business continuity plans, disaster recovery plans and procedures. The Contractor shall supply a copy of its business continuity policies and complete a CMHC Business Continuity Management Attestation Form prior to the execution of the Agreement and thereafter within thirty (30) days of CMHC's request.

ARTICLE XI. INDEMNIFICATION

SECTION 11.01 NDEMNIFICATION BY CONTRACTOR

The Contractor (the "Indemnifying Party") shall defend, indemnify, and hold harmless CMHC and each of CMHC's officers, directors, employees, agents, contractors, successors, and permitted assigns (each of the foregoing Persons, an ("CMHC Indemnitee")) from and against any and all Losses incurred by the CMHC Indemnitee arising out of or relating to any claim, suit, action or proceeding (each, an "Action") by a third party to the extent that such Losses do or are alleged to arise out of or result from:

(i)the Contractor's breach of any representation, warranty, covenant, condition, or obligation of the Contractor under this Agreement including, in the case of the Contractor, any action or failure to act by any Contractor personnel that, if taken or not taken by the Contractor, would constitute such a breach by the Contractor; or

(ii)any action or failure to take a required action or more culpable act or omission (including recklessness or willful misconduct) in connection with the performance or non-performance of any SaaS Services or other activity actually or required to be performed by or on behalf of the Contractor (including, in the case of the Contractor, any Contractor personnel) under this Agreement.

SECTION 11.02 INFRINGEMENT INDEMNIFICATION BY THE CONTRACTOR

The Contractor shall indemnify, defend, and hold each and all of the CMHC Indemnitees harmless from and against all Losses arising out of or resulting from any Action by a third party to the extent that such Losses do or are alleged to arise out of or result from a claim that any of the SaaS Services, or CMHC's or any Authorized User's use thereof, actually does or threatens to infringe, misappropriate or otherwise violate any Intellectual Property Right or other right of a third party, provided, however, that the Contractor shall have no liability or obligation for any Action or Losses to the extent that such Action or Losses arise out of or results from any:

(a) alteration or modification of the SaaS Services by or on behalf of CMHC or any Authorized User without the Contractor's authorization (each, a "CMHC Modification"), provided that no infringement, misappropriation, or other violation of third-party rights would have occurred without such CMHC Modification and provided further that any alteration or modification made by or for the Contractor at CMHC's request shall not be excluded from the Contractor's indemnification obligations hereunder unless (i) such alteration or modification has been made pursuant to CMHC's written specifications prepared independently of and without any contribution by the Contractor and (ii) the SaaS Services, as altered or modified in accordance with the CMHC's specifications, would not have violated such third-party rights but for the manner in which the alteration or modification was implemented by or for the Contractor;

(b) use of the SaaS Services by CMHC or an Authorized User pursuant to this Agreement in combination with any apparatus, hardware, software, or service not provided, authorized, or approved by or on behalf of the Contractor, if (i) no violation of third-party rights would have occurred without such combination and (ii) such apparatus, hardware, software, or service is not commercially available and not standard in the Contractor's or CMHC's industry and there are no specifications, Documentation or other materials indicating the Contractor's specification, authorization or approval of the use of the SaaS Services in combination therewith;

(c) access to or use of the SaaS Services that is expressly prohibited by this Agreement or otherwise outside the scope of access or manner or purpose of use described or contemplated anywhere in this Agreement or the Documentation;

(d) material breach of this Agreement by CMHC or material non-compliance herewith by any Authorized User; or

(e) violation of any applicable Laws by CMHC or any of its Authorized Users.

SECTION 11.03 MITIGATION

(a) If the Contractor receives or otherwise learns of any threat, warning or notice alleging that all, or any component or feature, of the SaaS Services violates a third party's rights, the Contractor shall promptly notify CMHC of such fact in writing and take all commercially reasonable actions necessary to ensure CMHC's continued right to access and use such SaaS Services and otherwise protect CMHC from any Losses in connection therewith.

(b) Subject to the exclusions set forth in 0(a) through 0(e), if any of the SaaS Services or any component or feature thereof is ruled to infringe or otherwise violate the rights of any third party by any court of competent jurisdiction, or if any use of any SaaS Services or any component thereof is threatened to be enjoined, or either Party's opinion, is likely to be enjoined or otherwise the subject of an infringement or misappropriation claim, the Contractor shall, at the Contractor's sole cost and expense:

   i. procure for CMHC the right to continue to access and use the SaaS Services to the full extent contemplated by this Agreement; or

ii. modify or replace all components, features, and operations of the SaaS Services that actually, or are likely or alleged to, infringe or otherwise violate the rights of any third party (" Allegedly Infringing Features") to end and avoid such infringement or violation while providing equally or more suitable features and functionality, which modified, and replacement services shall constitute SaaS Services and be subject to the terms and conditions of this Agreement.

iii. If neither of the remedies set forth in 0(b) is reasonably available with respect to the Allegedly Infringing Features, then the Contractor may direct CMHC to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that the Contractor shall: refund to CMHC any prepaid fees for SaaS Services that have not been provided; and in any case, at its sole cost and expense, secure the right for CMHC to continue using the Allegedly Infringing Features for a transition period of up to [NUMBER] (numeral) month[s] to allow CMHC to replace the affected SaaS Services or Allegedly Infringing Features without disruption.

(c) The remedies set forth in this 0 are in addition to, and not in lieu of, all other remedies that may be available to CMHC under this Agreement or otherwise, including CMHC's right to be indemnified pursuant to 0 and 0.

SECTION 11.04 INDEMNIFICATION BY CMHC

CMHC shall indemnify, defend, and hold the Contractor and its officers, directors, employees, agents, permitted successors and permitted assigns (each, a "Contractor Indemnitee") harmless from and against all Losses incurred by Contractor Indemnitee arising out of or resulting from any Action by a third party to the extent that such Losses do or are alleged to arise out of or result from:

(a) any claim that any CMHC Information is unlawful or actually does or threatens to infringe, misappropriate or otherwise violate any Canadian Intellectual Property Rights or other rights of any third party, provided, however, that CMHC shall have no liability or obligation with respect to any Action or Losses to the extent that such Action or Losses arise out of or result from any unauthorized access to or use, disclosure or other processing of CMHC Information, including Personal Information, by or on behalf of the Contractor, or through or enabled by the SaaS Services, whether authorized by the Contractor, due to a security breach or otherwise; or

(b) any use of the SaaS Services by CMHC or any Authorized User that is beyond the scope of or otherwise fails to conform to the express requirements or restrictions of this Agreement or any authorization or approval given in writing by the Contractor to CMHC or such Authorized User.

This 0 sets forth CMHC's sole obligation and liability and the Contractor's exclusive remedies with respect to any Action or Losses described therein.

SECTION 11.05 INDEMNIFICATION PROCEDURE

The Party seeking indemnification shall promptly notify the Indemnifying Party in writing of any Action for which it seeks indemnification pursuant to this 0 and cooperate with the Indemnifying Party at the Indemnifying Party's sole cost and expense. The Indemnifying Party shall immediately take control of the defence and investigation of such Action and shall employ counsel of its choice to handle and defend the same, at the Indemnifying Party's sole cost and expense. The Indemnifying Party shall not settle any Action on any terms or in any manner that adversely affects the rights of the other Party without the other Party's prior written consent which shall not be unreasonably withheld or delayed. Any Indemnitee may participate in and observe the proceedings at its own cost and expense with counsel of its own choice. A Party's failure to perform any obligations under this 0 will not relieve the Indemnifying Party of its obligations under 0 except to the extent that the Indemnifying Party can demonstrate that it has been prejudiced as a result of such failure.

ARTICLE XII LIMITATION OF LIABILITY

SECTION 12.01 EXCLUSION OF INDIRECT DAMAGES.

Except as otherwise provided in 0, in no event will either Party be liable under this Agreement for any consequential, incidental, indirect, exemplary, special or punitive damages.

SECTION 12.02 LIMITATION OF LIABILITY

Except as otherwise provided in 0, in no event shall either Party's liability under this Agreement exceed the greater of (i) fees paid and payable under this Agreement in the twenty (24) months preceding the event giving rise to the claim or (ii) the amount the Contractor is covered for in respect of the associated breach or loss under its insurance coverage as set forth in 0 of this Agreement.

SECTION 12.03 EXCEPTIONS

The exclusions and limitations in 0 and 0 shall not apply to:

(a) Losses arising out of or relating to a Party's failure to comply with its obligations under Article VII (Confidentiality and Privacy), 0 (article viii. Intellectual Property), or 0 (article x. Contingency Planning);

(b) a Party's indemnification obligations under 0 (section 11.01 ndemnification);

(c) Losses arising out of or relating to the Contractor's unauthorized suspension, termination or disabling of the SaaS Services in breach of this Agreement;

(d) Any amounts owed by a Party to the other Party pursuant to the Agreement;

(e) Losses arising out of or relating to a Party's gross negligence or more culpable conduct, including any willful misconduct or intentional wrongful acts;

(f) Losses for death, bodily injury, or damage to real or tangible personal property arising out of or relating to a Party's negligent or more culpable acts or omissions; or

Losses arising from or relating to a Party's violation of Laws.

ARTICLE XIII INSURANCE OBLIGATIONS

SECTION 13.01 INSURANCE REQUIREMENTS

The Contractor shall procure, supply, and maintain, at its own expense, the designated insurance, or cause to be procured and maintained such insurance in force for the duration of this Agreement. On the Effective Date, all insurance coverage(s) of the Contractor shall be issued by financially sound and responsible regulated insurance companies and shall have an A.M. Best Company, Inc. rating of "A-" or better (or such other debt rating agencies and/or rating as approved at the sole discretion of CMHC).

SECTION 13.02 COMMERCIAL GENERAL LIABILITY INSURANCE

Commercial General Liability insurance with an insurer licensed to do business in Canada with a limit of not less than five million dollars ($5,000,000) inclusive for personal injury, bodily injury (including death) and property damage for any one occurrence or series of occurrences arising from one cause. The policy shall provide coverage for, but not be limited to, all premises and operations of the Contractor, liability for products and completed operations, broad form coverage, contractor's liability, non- owned automobile, employer's liability, contractual liability, and liability specifically assumed under this Agreement. Canada Mortgage and Housing Corporation shall be added to the policy as an additional insured and the policy shall contain cross liability, and severability of interest clauses.

SECTION 13.03 TECHNOLOGY (ERRORS & OMISSIONS) LIABILITY

Technology Errors & Omissions Liability insurance with an insurer licensed to do business in Canada with a limit of not less than five million dollars ($5,000,000) per claim, providing coverage for, but not limited to, economic loss due to actual or alleged acts, errors or omissions or wrongful acts committed by the Contractor, its agents, or employees in the performance of services. The Contractor shall ensure that the policy is renewed continuously for a minimum period of three (3) years following the expiration or early termination of this Agreement and/or if the Contractor does not have Network and Privacy liability;

SECTION 13.04 COMPUTER SECURITY AND PRIVACY LIABILITY (ALSO KNOWN AS CYBER LIABILITY)

Computer Security and Privacy Liability with an insurer licensed to do business in Canada with a limit of not less than twenty million dollars ($20,000,000) per claim and aggregate, covering actual or alleged acts, errors or omissions committed by the Contractor, its agents, or employees. The policy shall also extend to include the intentional, fraudulent, or criminal acts of the Contractor, its agents, or employees. The policy shall expressly provide, but not be limited to, coverage for the following perils:

(a) unauthorized use/access of a computer system;

(b) defense of any regulatory action involving a breach of privacy or transmission of malicious code;

(c) failure to protect Confidential Information (personal and commercial information) from disclosure; and

(d) notification costs, whether or not required by statute.

The policy shall be renewed continuously for a minimum period of three (3) years following expiration or early termination of this Agreement.

The Contractor shall be responsible for all claims expenses and loss payments within the policy deductible or self-insurance retention. If the policy is subject to an aggregate limit, replacement insurance will be required if it is likely such aggregate will be exceeded. Such insurance shall be subject to the terms and conditions and exclusions that are usual and customary for this type of insurance.

If this insurance is provided on a claims-made basis, the Contractor shall maintain continuous insurance coverage during the term of this Agreement and in addition to the coverage requirements above, such policy shall provide that:

1. Policy retroactive date coincides with or precedes the insureds' initial services under the Agreement and shall continue until the termination of the Agreement (including subsequent policies purchased as renewals or replacements);

2. Policy allows for reporting of circumstances or incidents that might give rise to future claims; and

Not less than a three (3) year extended reporting period with respect to events which occurred but were not reported during the term of the policy or ongoing coverage is maintained.

Losses arising from or relating to a Party’s violation of Laws.

ARTICLE XIV OTHER CONDITIONS

SECTION 14.01 OTHER CONDITIONS

If there are material changes in the scope of SaaS Services provided under this Agreement, CMHC may request changes to the minimum insurance coverages set out above. All insurance policies required to be maintained by the Contractor pursuant to this insurance clause shall be primary with respect to this Agreement and any valid and collectible insurance of CMHC shall be excess of the Contractor’s

insurance and shall not contribute to it. All Certificate of Insurance shall mention that insurers will provide CMHC with at least thirty (30) days' written notice prior to cancellation of any insurance referred to under this insurance clause. In addition, the Contractor shall provide written notice to CMHC forthwith upon learning that an insurer described in this insurance clause intends to cancel or intends to make or has made a material change to, any insurance referred to in this insurance clause. A Certificate of Insurance meeting the above requirements shall be delivered to CMHC upon execution of this Agreement and for each renewal thereafter.

Without in any way restricting CMHC's discretion to grant or withhold its consent to a request to subcontract pursuant to this Agreement or any other contract, the Contractor agrees that it shall contractually obligate any subcontractor or independent contractor retained in connection with this Agreement and any other contract to maintain insurance against such risks and in such amounts that having regard to such subcontractor's or independent contractor's involvement in the provision of the SaaS Services could reasonably be expected to be carried by persons acting prudently and in a similar business to that of such subcontractor or independent contractor. It shall be the sole responsibility of the Contractor to decide whether or not any other insurance coverage, in addition to the insurance requirements stipulated herein, is necessary for its own protection or to fulfill its obligation under the Agreement.

SECTION 14.02 DISPUTE RESOLUTION

The Parties will make good faith efforts to first resolve internally within thirty (30) days any dispute, including over an invoice, in connection with this Agreement by escalating it to higher levels of management. Disputes will be governed by the jurisdiction of the applicable courts set forth in 0.

SECTION 14.03 NOTICE

All invoices and notices issued under this Agreement shall be in writing and shall be forwarded via mail, courier or e-mail:

1. To **CMHC** at the following address: [to be completed with the selected proponent]
2. To the **Contractor** at the following address: [to be completed with the selected proponent]

SECTION 14.04 CMHC REPRESENTATIVES

CMHC Managed Agreement

CMHC may appoint one or more CMHC employees or other personnel employed by CMHC as its Technical Representatives. The Contractor will be entitled to rely on all oral and written orders and instructions issued by any Contractor's Representative including, without limitation, instructions to initiate work, incur expenses and in management functions related to this Agreement on CMHC's behalf. CMHC reserves the right to select and reassign any CMHC Technical Representative. Furthermore, CMHC will remain responsible for its CMHC Technical Representative's performance of such services to the same extent as though such CMHC Technical Representatives were employees of CMHC.

SECTION 14.05 SURVIVAL

Provisions of these terms which by their nature should apply beyond the Term will remain in force after any termination or expiration of this Agreement including, but not limited to, the following provisions: Article III (Representations and Warranties), 0 (section 4.04 CMHC's Obligations upon Termination), 0 (section 4.05 Contractor's Obligations upon Termination), Article VII (Confidentiality and Privacy), 0 (Intellectual Property), 0 (article ix. Audit), 0 (Indemnification), 0

(article xii Limitation of Liability), 0 (Insurance), 0 (section 14.02 Dispute Resolution), 0 (section 14.18 Choice of Law), and this 0 (Survival).

SECTION 14.06 SEVERABILITY

If any term or provision of this Agreement is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability shall not affect any other term, provision of this Agreement, invalidate, or render unenforceable such term or provision in any other jurisdiction.

SECTION 14.07 WAIVER

Failure by either party to assert any of its rights under the Agreement shall not be construed as a waiver thereof.

SECTION 14.08 EQUITABLE REMEDIES

The Parties agree that irreparable damage would occur if any provision of this Agreement was not performed in accordance with the terms hereof and that the Parties are entitled to seek equitable relief, including injunctive relief or specific performance of the terms hereof, in addition to any other remedy to which they are entitled at law or in equity.

SECTION 14.09 CUMULATIVE REMEDIES

The rights and remedies under this Agreement are cumulative and are in addition to and not in substitution for any other rights and remedies available at law or in equity or otherwise.

SECTION 14.10 ASSIGNMENT

This Agreement shall not be assigned in whole or in part by the Contractor without the prior written consent of CMHC. No purported assignment of this Agreement shall relieve the Contractor from any obligation under this Agreement or impose any liability upon CMHC.

SECTION 14.11 SUCCESSORS AND ASSIGNS

This Agreement shall be binding upon the Parties, their heirs, executors, administrators, successors and assigns.

SECTION 14.12 CHANGES TO THE AGREEMENT

This Agreement may only be amended or modified in writing that specifically states that it amends this Agreement and is signed by an authorized representative of each Party.

SECTION 14.13 INDEPENDENCE OF THE PARTIES

It is understood by the Parties that the Contractor shall act as an independent contractor for the purposes of the Agreement. It and its employees, officers, agents and contractors are not engaged as employees of CMHC. The Contractor agrees to so advise its employees, officers, agents and contractors.

Without limiting the generality of the foregoing, the Contractor shall retain complete control of and accountability for its employees, agents and contractors. The Contractor shall prepare and process the payroll for its employees directly and shall withhold and/or pay all applicable employment taxes and statutory payroll deductions required in respect of its employees. All personnel employed by the Contractor at the beginning of the Term shall, at all times, and for all purposes, remain solely in the employment of the Contractor.

SECTION 14.14 CONTRACTOR'S AUTHORITY

The Contractor agrees that it has no authority to give any guarantee or warranty whatsoever expressed or implied on behalf of CMHC and that it is in no way the legal representative or agent of

CMHC and that it has no right or authority to create any obligation on behalf of CMHC or to bind CMHC in any way.

SECTION 14.15 NO PUBLIC ANNOUNCEMENTS

No Party to this Agreement shall make any public announcements in respect of this Agreement or the transactions contemplated hereby or otherwise communicate with any news media without the prior written consent of the other Party.

SECTION 14.16 SUBCONTRACTORS

1. The Contractor must obtain CMHC's written consent, which may be given or withheld in CMHC's sole discretion, prior to entering into agreements with or otherwise engaging any person or entity, including all subcontractors and affiliates of the Contractor, other than the Contractor's employees, to provide any SaaS Services to CMHC. Each such approved subcontractor or other third party, a "Permitted Subcontractor".
2. CMHC's approval shall not relieve the Contractor of its obligations under the Agreement, and the Contractor shall remain fully responsible for the performance of each such Permitted Subcontractor and its employees and for their compliance with all of the terms and conditions of this Agreement as if they were the Contractor's own employees.
3. Nothing contained in this Agreement shall create any contractual relationship between CMHC and any of the Contractor’s subcontractor, supplier, employee, officer, director, or agent;
4. The Contractor shall require each Permitted Subcontractor to be bound in writing by the confidentiality provisions of this Agreement, and, upon CMHC's written request, to enter into a non-disclosure or intellectual property assignment or license agreement in a form that is reasonably satisfactory to CMHC before sharing any information with relation to the SaaS Services;
5. The Contractor shall ensure that all persons, whether employees, agents, subcontractors, or anyone acting for or on behalf of the Contractor, are properly licensed, certified, or accredited as required by applicable Laws and are suitably skilled, experienced, and qualified to perform the SaaS Services.

SECTION 14.17 NO THIRD-PARTY BENEFICIARIES

This Agreement is for the sole benefit of the Parties hereto and their respective successors and permitted assigns and nothing herein, express, or implied, is intended to or will confer upon any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Agreement.

SECTION 14.18 CHOICE OF LAW

This Agreement shall be governed by and construed in accordance with the Laws of the Province of Ontario and the Laws of Canada as applicable. The Parties attorn to the jurisdiction of the Federal Court or the courts of the Province of Ontario as appropriate in the circumstances. The Contractor shall give all notices and obtain all licenses, permits and authorizations required to perform the SaaS Services. The Contractor shall comply with all the Laws applicable to the services or the performance of this Agreement.

SECTION 14.19 COUNTERPARTS

This Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this Agreement delivered by facsimile, email or other means of electronic transmission is deemed to have the same legal effect

as delivery of an original signed copy of this Agreement, if the Party sending the facsimile, email or other means of electronic transmission has received express confirmation that the recipient Party received the Agreement (not merely an electronic facsimile confirmation or automatic email reply).

SECTION 14.20 FORCE MAJEURE

In the event that a Party is prevented from fulfilling its obligations under the terms of this Agreement by a force majeure or act of God (an event or effect that cannot be reasonably anticipated or controlled), the impacted Party shall notify the other Party in writing as soon as reasonably possible. The written notice shall be sent by registered mail or email and shall outline the circumstances that constitute a force majeure or an act of God, which may include, but are not limited to, war, serious public disturbances, epidemic, impediments arising from orders or prohibitions of public authority, actions of public enemies, strikes, lockouts and other labour disputes, riots, flooding, hurricane, fire, explosion or any other natural disasters over which the Party has no reasonable control. The Contractor's economic hardship or changes in market conditions are not force majeure events. The Contractor shall use all diligent efforts to end the failure or delay of its performance, ensure that the effects of any force majeure event are minimized and resume performance under this Agreement.

Where CMHC concludes, in its sole discretion, that the Contractor will not be able to fulfill its obligations under this Agreement, CMHC may terminate this agreement and, or secure the services of other contractors to perform the SaaS Services without further compensation, penalty or obligation to the Contractor.

SECTION 14.21 HEADINGS

The clause headings used herein are inserted only as a matter of convenience and for reference and shall not affect the construction or interpretation of the Agreement.

SECTION 14.22 LANGUAGE

CMHC as a federal crown corporation is governed by the Official Languages Act and as such must provide services to the public in both official languages, English and French. Any communication with CMHC and CMHC third parties (i.e. claimants), shall be provided in the official language chosen by the individual receiving the service. Therefore, the Contractor acting on behalf of CMHC must be capable of providing services and products in both official languages to all CMHC locations.

SECTION 14.23 ORDER OF PRECEDENCE

The documents comprising the Agreement are complementary and what is called for in any one shall be binding as if called for by all. The Agreement documents shall be interpreted as a whole and the intent of the whole shall govern. In the event of any inconsistency between this Agreement, the related Schedules, exhibits, attachments and appendices and any other documents incorporated herein by reference, the following order of precedence governs: (i) the terms and conditions of this Agreement; and (ii) any Schedules, exhibits, attachments and appendices and any other documents incorporated herein by reference to this Agreement.

SECTION 14.24 ENTIRE AGREEMENT

This Agreement contains all of the agreements of the Parties and no other representations or warranties, verbal or otherwise, exist between the Parties. In case of conflicts between the Contractor's documents and CMHC's documents, CMHC’s shall govern.

This Agreement, including any documents incorporated herein by reference, constitutes the sole and entire agreement of the parties, and supersedes all prior or contemporaneous understandings, written or oral. These terms prevail over any terms and conditions contained in any other

documentation and expressly exclude any of the Contractor's general terms and conditions or any other document issued by the Contractor in connection with this Agreement, not incorporated herein.

No Shrink-Wrap. Only terms which are presented in full and directly described herein will form part of this Agreement. Any terms or conditions that are purported to be incorporated by reference through URLs, read me files or otherwise, shall not form part of this Agreement. CMHC is not bound by and does not accept any "shrink-wrap" or "click-wrap" conditions or any other conditions, express or implied, that are contained in or on the SaaS Service provided under the service packaging or conditions that may accompany the SaaS Service in any manner, regardless of any notification to the contrary from the Contractor or any associated third party. For greater clarity, the Contractor agrees that CMHC is not bound by and does not accept any "shrink-wrap" or "click-wrap" conditions or any other conditions, express or implied, that are contained on the Contractor's Internet site or conditions that may accompany the SaaS Service in any manner, regardless of any notification to the contrary.

[Signature follow on the next page]

IN WITNESS WHEREOF:

This Agreement has been executed by duly authorized officers of the Parties as follows:

SELECTED PROPONENT LEGAL NAME	**CANADA MORTGAGE AND HOUSING CORPORATION**
_____	_____
Signature	Signature
_____	_____
Name and Title	Name and Title
_____	_____
Date	Date

I have the authority to bind the Contractor.

SCHEDULE A

SAAS SERVICES

TO BE COMPLETED AND AGREED UPON WITH THE SELECTED PROPONENT.

Capitalized terms used but not defined in this Schedule A have the meaning ascribed to them in the Agreement.

1. Description of SaaS Services and Specifications
2. Implementation Plan Deliverables
3. Documentation
4. Authorized User(s):
5. Service Levels and Support

SCHEDULE B

FEES

TO BE COMPLETED AND AGREED UPON WITH THE SELECTED PROPONENT.

Contractor Tax Forms

In accordance with section 5.06 of this Agreement, the Contractor may use the following link to retrieve the latest tax form: https://www.canada.ca/en/revenue-agency/services/forms-publications/forms/t1204.html

In accordance with section 5.06 of this Agreement, the Contractor shall complete the following Vendor Information Form:

VENDOR INFORMATION FORM

All new vendors must complete all sections of this form, unless otherwise indicated.
This applies also to existing vendors who need to amend their information.

CMHC USE ONLY
Vendor No.
CMHC No.

☐ NEW VENDOR ☐ AMEND EXISTING VENDOR

PART A - IDENTIFICATION

Legal Name of Entity or Individual	Operating Name of Entity or Individual (if different from Legal Name)

Suite/Apt No.	Street Address	City	Province	Postal Code

Telephone Number	Fax Number	E-mail (for payment remittance notification)

PART B - TYPE OF CONTRACT (required for T1204 reporting under the Income Tax Act)

Please select ONE of the following:

☐ Contract for goods only ☐ Contract for mixed goods and services ☐ Contract for services only ☐ Contribution / Loan (If selected, go to Part D)

PART C - STATUS OF CONTRACTOR (required for T1204 reporting under the Income Tax Act)

☐ Sole Proprietor (If yes, provide name):	Last Name	First Name	Initial

☐ Corporation ☐ Partnership (If yes, provide filer identification number.)

BN (Business Number)	SIN (If sole proprietor and no Business Number)	GST/HST No. (If registered)	QST No. (If registered)

PART D - PAYMENT INFORMATION All payments will be made to the account identified below.

For accounts in CAN$

☐ Direct Deposit (EFT) (**CMHC's preferred option**) ☐ Wire ☐ Cheque (exceptional circumstances)

For direct deposit or wires, please provide the following information and attach a void cheque or equivalent.
This account must hold Canadian funds at a financial institution in Canada.

Name of Account Holder	Bank Transit No. (5 digits)	Financial Institution No. (3 digits)	Bank Account No.

Financial Institution Name	Branch Street Address	City	Province	Postal Code

For accounts in foreign currency CMHC will make the payment through a wire.
CMHC is not responsible for wire fees charged to the vendor by their financial institution.
The information required will vary depending on the country.

Name of Account Holder	Bank Account No.	Swift code (Bic)	Routing #	IBAN

Financial Institution Name	Financial Institution Address

PART E - CERTIFICATION

I certify that the information provided above is correct and complete, and fully discloses the identification of this vendor.
I request and authorize Canada Mortgage and Housing Corporation to make all payments payable to me to the account identified in Part D.

Name	Title	Telephone Number

Signature	Date

PART F - CMHC CONTACT

Name	Title	Department

PART G – ADDITIONAL INFORMATION REQUIRED FOR SPECIFIC CMHC PROGRAMS

Select legacy system:

☐ AHPS ☐ PMSH ☐ MICS

Other information:

Submit the completed form and any inquiries to Shared Services at: VendorReq@cmhc.ca

Canada

Disponible en français - 68965

Page 1 of 1

CMHC SCHL

SCHEDULE C

PRIVACY AND SECURITY REQUIREMENTS

"**Authorized Person**" means officers, employees and contractors of the Contractor who have a need to know to the Information.

"**Data Custodian**" means the Contractor or the Contractor subcontractor who is granted access to CMHC Information and assumes the responsibilities set out in **Exhibit 1 to this Schedule C** of this Agreement

"**Identified Person**" means an Authorized Person whose current work-related responsibilities require access to the CMHC Information.

"**Logical Access Controls**" means the process of enforcing proper identification, authentication and accountability with respect to access to a computer system, based on the latest information technology (IT) security guidance. These include:

(a) individual user accounts;

(b) complex passwords eight (8) characters minimum, lower and upper case, numbers, special characters);

(c) access-based on role (privileged vs. non-privileged); and

(d) auditing.

"**Portable Storage Devices (PSDs)**" means devices that are portable and contain storage or memory into which users can store information, including, but not limited to, laptops, CD-ROMs, flash memory sticks, backup media and removable hard disks.

"**Protected B**" means a security level assigned to information or assets that, if compromised, could cause serious injury to an individual, organization or government.

"**System**" means a single IT-related device, a component of such a device or a group of IT-related devices that may be used to receive, store, process or transmit information. This includes, but is not limited to, personal computers, servers, laptops, tablets, smart phones, virtual computers and cloud based virtual systems.

"**Visitor**" means an individual, other than an Authorized Person, who has been invited into the secure area by an Authorized Person, as permitted by the Contractor's access policies.

Privacy and Security Requirements

The Parties are required to protect the CMHC Information in accordance with applicable direction and guidelines from the Treasury Board of Canada ("TBS"), or their equivalent in the case of the Contractor, with respect to the protection of "Protected B" data, including guidance from CSE (ITSG-33) which aligns with the ISO 27001 framework. Further as a federal government institution, the Contractor acknowledges that CMHC is subject to the *Access to Information Act* (Canada) and the *Privacy Act* (Canada) and therefore the Contractor agrees to submit to whatever measures are necessary in order to ensure that CMHC can comply with these Laws and their related regulations, policies, and directives ("ATIP Legislation").

As such, the Contractor agrees: (i) to protect any Personal Information that it may access from CMHC Information provided through this Agreement in a manner that is compatible with provisions of ATIP Legislation; and (ii) will ensure that it has in place appropriate privacy protection measures to safeguard all CMHC Information that it has access to under this Agreement. More specifically, the

Contractor shall, as required by the provisions of Article VII of this Agreement, comply with the security requirements described below at all times:

Physical Access:

(a) CMHC Information will be accessed within a secure location that allows unescorted access only to Authorized Persons. All Visitors to the secure location will be escorted by an Authorized Person at all times. The secure location can be within a series of buildings, one entire building, an entire floor within a building, or a single room. Once the perimeter of the secure location is defined, these requirements apply to all areas within the perimeter. Where a series of buildings is involved, a secure perimeter will be defined for each building. CMHC may approve other secure environments that provide a similar level of protection to CMHC Information.

(b) Access to CMHC Information is limited to Identified Persons. The duties of the Data Custodian, as stated in **Exhibit 1 to this Schedule C**, include maintaining an auditable trail on access to CMHC Information by Identified Persons. Under no circumstances may Visitors be permitted to access CMHC Information.

IT Storage and Transmission:

(c) The Contractor shall ensure that CMHC Information remain in Canada and expressly agrees to logically segregate CMHC Information that is in electronic form and physically segregate CMHC Information in physical form. All Systems with access to CMHC Information will employ Logical Access Controls at the device and network level and will have functional and current antivirus software.

(d) Where CMHC Information is held on PSDs, complex passwords with encryption will be used. The encryption level will meet the latest communications security establishment standards for "Protected B" information which aligns with the ISO 27001 framework. This applies equally to backups of CMHC Information stored on PSDs.

(e) Servers storing and transmitting unencrypted data, where used, will be located in a secure, controlled-access area, preferably in the same area where CMHC Information is accessed. If located in a separate area, controls will be in place to ensure that only Identified Persons can access the server. Unless CMHC Information is encrypted continuously while outside the secure area, a conduit will be used for all cabling and all cross-connect areas will be physically secured.

(f) Network firewall rules will be in place such that no System processing CMHC Information can communicate at the network layer with any system that can be accessed by non-Identified Persons.

(g) Network firewall rules will also be in place such that no System processing CMHC Information can be accessed at the network layer by a System outside of the secure area. CMHC Information may be stored on and transmitted over networks not meeting these requirements, provided that it is encrypted, except when at rest and in use by an Identified Person. Alternatively, CMHC Information may be stored on a stand-alone computer in a secure area with no external connections, or on a closed network within the secure area. When the network transmits information that leaves a secure area (for example, when a series of buildings house employees within a single organization), the CMHC Information will be encrypted whenever it is outside the secure area.

Physical Storage:

(h) When not in use, PSDs containing CMHC Information will be stored in secure containers. This applies equally to backups of CMHC Information.

(i) CMHC Information will not be removed from the secure area (as described in point 1 above) in any format (e.g., printouts, PSDs, etc.), and in accordance with this Schedule C. When not in use, printed documents containing CMHC Information will always be stored in secure containers.

Information Copying and Retention & Record Management:

(j) Copies and extracts of CMHC Information may only be made for the purposes of carrying out the permitted purposes as covered by this Agreement. When no longer needed, any such copies or extracts will be destroyed in a secure manner as required under Article VII of this Agreement (as applicable).

(k) Paper documents containing CMHC Information will be destroyed (shredded) in a secure manner before disposal. All electronic storage media used in the processing of CMHC Information, including all back-up, PDSs, photocopiers and other electronic media where CMHC Information has been electronically stored, will be sanitized or destroyed, in accordance with the latest communications security establishment standards for "Protected B" information when disposing of such media, or when return or destruction of CMHC Information is required pursuant to Article VII of this Agreement (as applicable).

(l) The Contractor's Data Custodian agrees to establish and maintain an inventory of all data files received from CMHC, as stated in **Exhibit 1 to this Schedule C**.

Privacy Program:

(m) The Contractor shall ensure that it has appointed a Chief Privacy Officer (or equivalent) who is accountable for the Contractor's privacy program and compliance with its privacy requirements and who shall be promptly available to address privacy questions or concerns raised by CMHC.

(n) The Contractor shall ensure it has implemented a privacy policy that addresses its compliance with privacy requirements under applicable privacy legislation.

(o) The Contractor shall ensure it provides mandatory privacy awareness training and education to any individuals who may be involved in the delivery of services to CMHC under this Agreement. Such training must be periodically reviewed and updated, as required.

(p) The Contractor shall conduct regular privacy assessments to ensure it is meeting its privacy requirements under applicable privacy legislation. Upon CMHC's request, these assessments will be made available to CMHC, and the Contractor shall address any gaps in its privacy program related to the performance of this Agreement as may be reasonably required by CMHC.

(q) The Contractor shall assist CMHC, as reasonably required, in any Privacy Impact Assessment (PIA) or other similar privacy assessment undertaken by CMHC related to the services provided to CMHC under this Agreement.

EXHIBIT 1 TO SCHEDULE C

RESPONSIBILITIES OF THE DATA CUSTODIAN

The Data Custodian, designated by the Contractor will implement the following requirements:

1. Prepare a document for the use of the Contractor's employees and contractors engaged by the Contractor, outlining the terms and conditions governing the use of CMHC Confidential Information, as well as the procedures to send, receive, handle and store CMHC Confidential Information (hereinafter the "Confidentiality Document"). The Confidentiality Document will include the following terms and conditions of this Agreement:

   a) Confidentiality of CMHC's Confidential Information, as specified in the Agreement;

   b) Use of CMHC's Confidential Information, as specified in the Agreement;

   c) Access to CMHC's Confidential Information, as specified in the Agreement; and

   d) Security Requirements as specified in the Agreement

   (k) Prior to granting access, the Data Custodian will ensure that every employee and every contractor engaged by the Contractor who accesses CMHC Information has agreed in writing to comply with confidentiality terms no less strict than this Agreement.

   (l) Maintain a register of all Identified Persons who have been granted access to the data files received from CMHC by the Contractor, containing the following information:

   a) File name and reference period;

   b) Name of employee or/and contractors engaged by the Contractor to whom access is given;

   c) Justification for access;

   d) Name of delegated manager who authorized access and date of authorization; and

   e) Start and end dates of period for which access is authorized.

APPENDIX E – PRIVACY AND SECURITY CONTROLS QUESTIONNAIRE

	PRIVACY PRINCIPLE	PRIVACY / SECURITY CONTROLS	RESPONSE/CONFIRMATION OF EXISTING CONTROLS ******Please provide detailed responses******
1.	Accountability	1.1 Designated Privacy team: Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the organization's privacy policies and procedures. Demonstrate adherence to leading industry frameworks such as PIPEDA	
		1.2 Internal Oversight: Describe your internal processes for monitoring adherence to your privacy policies and procedures.	
		1.3 Training & Awareness: Describe your privacy and security training and privacy awareness / upskilling programs for staff.	
		1.4 Third-Party / Vendor Management: How do you oversee third-party / vendors or subcontractors for privacy adherence and ensure compliance to CMHC's terms, agreements, and requirements?	
		1.5 Communicate Changes: Is there a process for notifying CMHC if there are new or changed arrangements	

		with third parties or sub-contractors accessing Personal Information?	
		1.6 History of Sharing: How do you maintain a history of Personal information sharing – including dates and categories of information transferred, to whom and where it was transferred, and the purpose?	
		1.7 Global Compliance: Do you adhere to other jurisdictional privacy laws (e.g., GDPR, CCPA)? Provide evidence or certifications of compliance.	
2.	Identifying Purposes	2.1 Purpose Determination & Documentation: Describe the processes and criteria your organization uses to determine and document the purposes for which personal information is collected, used, or disclosed.	
3.	Consent	3.1 Obtaining Consent: Describe how you obtain consent for the collection, use, or disclosure of personal information. Include processes for both implicit and explicit consents.	
4.	Limiting Collection	4.1 Data Minimization: Describe your measures to ensure that only the necessary personal information is collected.	
5.		5.1 Use & Disclosure:	

	Limiting Use, Disclosure, and Retention:	How do you ensure personal information is only used or disclosed for the purposes initially intended?	
		5.2 Retention and Storage: Explain your retention policies, processes, schedule, and monitoring.	
		5.3 Secure Disposition: How do you securely return, dispose of, destroy or de-identify personal information that is no longer required?	
6.	Accuracy	6.1 Data Quality: Describe how you ensure the personal information you hold is accurate, complete, and up-to-date.	
7.	Safeguards	7.1 Security in Privacy Policies: The organization's privacy policies (including any relevant security policies), address the security of Personal Information.	
		7.2 Protection Measures: Describe the technical, physical, and administrative security measures protecting personal information. Please detail mechanisms such as: - Biometrics - Firewalls & Intrusion detection systems - VPNs - Session time-out securities - Data encryption methods	

		- Audit trails	
		7.3 Security Assessments: Explain how you meet security controls for up to and including Protected A or B as per Government of Canada standards, such as or equivalent to: - ISO27001:2013 - ITSG-33 - SOC 1 Report - SOC 2 Report - CSEA 3416 - SSAE 18 Alternatively, if you are using a third-party provider to manage your network (such as Bell Canada or Rogers or Microsoft), SOC reports are available through your provider and will satisfy this requirement.	
		7.4 Logical Access to Personal Information: Explain how Logical access to Personal Information is restricted by procedures that address the following matters: a) Authorizing and registering internal personnel and individuals; b) Identifying and authenticating internal personnel and individuals; c) Making changes and updating access profiles; d) Granting privileges and permissions for access to IT	

		infrastructure components and Personal Information; e) Preventing individuals from accessing anything other than their own personal or sensitive information; f) Limiting access to Personal Information to only authorized internal personnel based upon their assigned roles and responsibilities using techniques such as access management, de-identification ; g) Distributing output only to authorized internal personnel; h) Restricting logical access to offline storage, backup data, systems, and media; i) Restricting access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls); and j) Preventing the introduction of viruses, malicious code, and unauthorized software. k) Preventing co-mingling of personal information collected from this initiative with that of other organizations.	
		7.5 Physical Access Controls: How physical access to Protected A or B information is restricted	
		7.6 Environmental Safeguards: Explain how personal information, in all forms, is protected against accidental Disclosure due to natural disasters and environmental hazards.	

		7.7 Incident Management: Does your organization have an incident management policy and process that includes defined processes for problem identification, risk mitigation, remediation, and timely notification to CMHC upon discovery? Have you had any data breaches (material breaches with a risk of harm and that were reported to TBS or OPC) in the past 24 months? If so, provide details on the incident and corrective measures taken.	
		7.8 Data Residency Do you have the infrastructure to store Personal Information collected as part of the CMHC initiative inside Canada? Protected Information must reside in Canada at all times.	
		7.9 Testing Security Safeguards How do you test the effectiveness of the key administrative, technical, and physical safeguards protecting Personal Information are conducted periodically including a Threat and Risk assessment (TRA) Penetration testing, or similar security assessment.	
8.	Openness	8.1 Policy Availability: Can you ensure that information about an organization's privacy policies and procedures, including the name of the Privacy Officer and their responsibilities, are user-friendly, communicated and made readily available to the public, internal personnel and third parties who need them. Please share them with CMHC.	

9.	Individual Access	9.1 Access & Correction: Describe the process for individuals to access their personal information in your organization and correct inaccuracies.	
10.	Challenging Compliance	10.1 Complaints Process: Describe the process in place for individuals to challenge your organization's compliance with privacy principles.	

APPENDIX F – BUSINESS CONTINUITY AND DISASTER RECOVERY ATTESTATION FORM

PART A

Company Name: XXXXXXXX Contract #: XXXXXXXX

1. Please identify your Business Continuity & Disaster Recovery Contact Person. (Primary and alternate).

_____ Name (Primary)	_____ Name (Alternate)
_____ Title	_____ Title
_____ Mailing Address	_____ Mailing Address
_____	_____
_____ Telephone number	_____ Telephone number
_____ E-mail Address	_____ E-mail Address

	2. Please confirm (and where possible provide documentation) that the Business Continuity and Disaster Recovery Plans for the business functions/services you provide to CMHC is current and meets the following requirements:	**Yes**	**No**
a.	The plans are developed to maintain the current service level agreement/contract in any circumstances which may have a significant impact on your organization;		
b.	The plans address worst case scenario(s), including drastic reductions (up to 50%) of your workforce;		
c.	The plans are scoped to include technology failures such as prolonged outages (this should change in accordance with the Recovery Time Objective (RTO) in the contract), loss of systems such as hardware failures, computer viruses, etc.		
d.	The plans are scoped to include natural disasters, terrorist attacks, etc.		

e.	The plans include a comprehensive Business Impact Analysis (BIA);		
f.	The plans include communication strategies and critical contact names and telephone numbers;		
g.	The plans include notification mechanism to CMHC, should these changes impact your ability to perform the contracted business functions;		
h.	The plans are maintained, reviewed, and approved at least annually at an appropriate management level		
i.	The plans are exercised at least annually; If yes, please provide the following information about the latest exercise: **Business Continuity:** Date: Type: Result: **Disaster Recovery:** Date: Type: Result:		
3.	**Please confirm (and where possible provide documentation) whether the business functions/services you provide to CMHC have been sub-contracted.**		
4.	**Please confirm that the sub-contractor's Business Continuity and Disaster Recovery Plans meets the requirements outlined in two, above.**		
5.	**I identify and attest that all dependencies including our 3rd party service providers support the current service level agreements/contracts with CMHC and recognize that full compliance must be maintained at all time.**		

If the above response is 'No', please provide justification:

_____
_____
_____
_____

Completed by Service Provider Senior Executive Officer (or delegated authority)

Executive Officer Name *(Printed)*: _____

Executive Officer Title *(Printed)*: _____

_____

Signature Executive Officer: _____

Date: _____

PART B

Validation (to be completed by CMHC)

1. Based on the results noted in this Report on Outsourcing Compliance dated [*insert date*], [*insert provider name*] asserts the following compliance status (*check one*):

☐ **Compliant** (All CMHC requirements are met)

☐ **Non-Compliant** (Some CMHC requirements are met)
Target Date for Compliance: _____

Completed by CMHC BCM Lead (or delegated authority)

CMHC BCM Name *(Printed)*: _____

CMHC BCM Title *(Printed)*: _____

Signature BCM Lead: _____

Date: _____