Canada Mortgage and Housing Corporation
Société canadienne d'hypothèques et de logement

CMHC SCHL

cmhc.ca

Proponent Questions and CMHC Responses (Q&As)

RFP 002376 – Governance, Risk & Compliance (GRC) Solution

Date: March 14, 2024

Q&A 3

Q&A TABLE

No.	Proponent's Question	CMHC Response
1	Can we submit two separate proposals in order to provide CMHC with two separate GRC solution options?	Each system would have to be in a separate submission and will be evaluated separately.
2	Please enlist and briefly describe the technical infrastructure, technology, and tools currently involved in different data lifecycle stages. From data creation or ingestion to data destruction or archiving by different roles, including analytics, data stewards, BI users, etc.	CMHC will not provide this information at this time.
3	Please enlist and describe high data availability and disaster recovery scenarios, methodologies, methods, and tools currently in place, including geo-distribution and multi-tenancy.	CMHC will not provide this information at this time.
4	Could you please describe data in current systems in terms of the following: • Volume – the amount of data (Tb, records, entities, transactions, unique users and customers, and any other corresponding measures);	The only system being replaced by the proposed GRC is the audit system (TeamMate+). CMHC has approximately 225 historical projects in TeamMate+ and no other significant legacy data (risk/control data) that needs to be migrated for audit. The database file size is approximately 40 GB.

	• Variety – the number of different types and kinds of data (data domains, entities, attributes); • Velocity – speed of data generating, changing, and processing (GB, records, transactions per year, month, day, hour, second);	CMHC is only migrating an active data set (approximately 10 years of data).
5	Are there any data retention policies in place?	Audit and Risk records see 4.4.1 g – retention period of 10 years after record was last modified.
6	Please enlist and briefly describe the roles, business and technical, involved in different stages of the data lifecycle for current systems.	CMHC will not provide this information at this time.
7	Please enlist and describe, if needed, the current ways to access data. Like integrated desktop applications, web portals, mobile applications, chatbots, embedded analytics, e-mails, specific hardware, or anything else.	CMHC will not provide this information at this time.
8	Are there any limitations related to migration - like availability and duration of possible downtimes?	The migration of audit data is expected to occur as part of implementation of the new system and will consist mostly of migrating historical data. As such, expectations are that there wouldn't be any significant restrictions required related to availability/downtimes during the migration.
9	In our experience responding to similar Government of Canada solicitations for SaaS solutions, there are typically functional and non-functional mandatory requirements to ensure that bidders are compliant. In addition, the Government of Canada Software as a Service Supply Arrangement (SaaS RFSA) provides a set of mandatory security requirements approved by the Canadian Centre for Cyber Security (CCCS) in order to assess a Protected B SaaS	CMHC Security is supportive of Proponents providing evidence of additional security solutions in their RFP submissions. CMHC will not be amending the Mandatory Requirements.

	offering (Link to posting: RFSA - SaaS Method of Supply (GC Cloud) - Tender Notice | CanadaBuys). Would the Crown consider adding the Mandatory requirements approved by CCCS for Protected B SaaS solutions as seen in the Government of Canada SaaS RFSA (Solicitation number EN578-191593/F)?	
10	For Protected B SaaS solutions, the Canadian Centre for Cyber Security (CCCS) requires SaaS vendors to provide compliance with the following industry recognized certifications and audit reports. ○ ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; and ○ ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services; and ○ ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors ○ Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality. Would the Crown consider adding a Mandatory requirement for vendors to provide these certifications with bid submission to demonstrate compliance with the requirement for Protected B SaaS?	CMHC Security is supportive of Proponents providing evidence of additional security solutions in their RFP submissions. CMHC will not be amending the Mandatory Requirements.

11	For Rated requirement R1.7 under the section Experience and qualifications of the organization in the RFP, can the Crown confirm the following: a. If Bidders are required to provide SOC 2 Type II reports? b. If Bidders can provide the summary page of the report In lieu of the entire report? (due to sensitive information the report is typically not shared).	A full SOC 2 Type II report is not required. Proponents can provide a summary page detailing proof/validation they meet the requirements of certification/attestation.
12	For Rated requirement R1.4 under Experience and qualifications of the organization, can the Crown provide a definition of what is considered a large complex organization? (i.e., based on number of employees, annual revenues etc.)	At this time, CMHC is not assigning a prescriptive definition to "large complex organization". Proponents are encouraged to use their own determination in accordance with Rated Requirement 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."
13	Section 2.2.1 Scoring by the Evaluation Team of the RFP provides a table with a breakdown of how the rated criteria are scored. Can the Crown confirm that each rated criteria under the rated sections R.1 Experience and Qualifications of the Organization, R.2 Approach and Methodology and R.3 Experience and Qualification of the Proposed Resource(s) are worth a maximum of 5 points each as set out in the scoring table in Section 2.2.1?	The rated criteria (R.1-R.4) and the Presentation will be evaluated using the scoring grid provided in Section 2.2.1. The weighting for the rated criteria is set out in the RFP, Section J (and updated via Amendment No. 2). For clarity, R.1. is weighted at 5%, R.2. is weighted at 10%, and R.3. is weighted at 5%.

14	To ensure fairness and transparency to all vendors, can the Crown confirm if each sub requirement within the rated sections R.1 - R.3 are weighted equally? For example, R.1 Experience and Qualifications of the Organization has 11 sub requirements presumably worth 5 points each, therefore each requirement is worth 1/11 of the total 5% of that section.	For the Rated Criteria (R.1., R.2., and R.3.) the subcategories will be evaluated following the scoring matrix (0-5) as provided in Section 2.2.1 of the RFP. The subcategory scores will be averaged to provide the overall score for the Rated Criteria (R.1., R.2., and R.3.).
15	In the Pricing Form Table 1 - Item 3 Annual Fees, can the Crown please confirm if its annual pricing (to be in line with Item 4) and if the quantity needs to be 3 for the 3 year initial period?	For the Annual Cost, the quantity (QTY) should be three (3) and the UNIT COST would be the Annual Fee. The TOTAL CDN BEFORE TAX would be the subtotal (i.e. QTY X UNIT COST = TOTAL CDN BEFORE TAX).
16	In the Pricing Form Table 1 - Item 4 Ongoing support costs, given that the Crown requires an annual price and the table is for 3 years, would the crown consider updating the pricing table for hard coding 3 as the quantity?	For the On-going Support Costs, if not included in Item No. 3 – Annual Fees, the quantity (QTY) should be three (3) and the UNIT COST would be the annual fee for On-Going Support Costs. The TOTAL CDN BEFORE TAX would be the subtotal (i.e. QTY X UNIT COST = TOTAL CDN BEFORE TAX).
17	In the Pricing Form Table 1 - Item 5 Training, is training to be considered a one-time cost for the implementation period?	Yes, this is a one time cost.
18	Can the Crown confirm if the total value of Table 1 in the Pricing Form needs to be the total value of all costs for the initial 3 year period?	Yes, the Sub-Total for Table 1 in the Pricing Form must be inclusive of all costs the proponent intends to charge for the duration of the three (3) year Initial Term of the Agreement.
19	Based on the latest Amendment for the evaluation and ranking of proponents, we would like to validate our understanding below: a) The scores for (i) Stage II (B) RATED CRITERIA and (ii) Stage III PRICING will be evaluated and the top four	Yes. This interpretation is correct.

	ranked proponents will proceed to the next stage - Stage IV Presentation; b) Following the presentation, the top four ranked proponents will be evaluated and scored based on the presentation criteria set out in the amended Section K - Presentation; c) The Vendor who scores the highest in the Presentation stage will receive a written invitation to enter into direct contract negotiations Can the Crown confirm our understanding of the process and ranking of proponents?	
20	For Requirement 4.4.3, can the Crown provide an example of an audit project?	Audit projects are conducted by CMHC's independent Internal Audit function, with the objective of providing the CMHC Board and Senior Management with independent, risk-based, and objective assurance, advice and insight. Audit projects are generally focussed in the areas of governance, risk management and internal control across the CMHC internal audit universe (e.g., business activities, processes, programs, risk areas, etc.).
21	Under Section 4.3.3 Assessments, can the Crown provide an example of a risk hierarchy?	A risk hierarchy or taxonomy is a comprehensive, common, and stable set of risk categories that is used within an organization. By providing a *comprehensive* set of risk categories, it encourages those involved in risk identification to consider all types of risks that could affect the organization's objectives. Examples are the ORX reference taxonomy and BASEL II event types.

22	Under Section 4.6.5 – can the Crown provide additional information about the Personal Information Bank?	Infosource is the CMHC PIB. It is a PDF list published on CMHC external website - INFO SOURCE 2023 - Sources of Federal Government and Employee Information (cmhc-schl.gc.ca) GRC should be able to track for each program/product the following information: - if personal information (PI) is involved, - PIB number, - retention code, - link to the Privacy Impact Assessment Examples on the CMHC website: • Info source 2023PDF • Info Source 2023PDF
23	Query regarding the Procurement Business Number (PBN). I have registered on the https://mu.ariba.com/profile/org-profile to get the number. Is this correct or something else has to be done to get the PBN.	Registration with SAP Ariba is comparable to the PBN registration for doing business with the Government of Canada. Registration with Public Services and Procurement Canada ("PSPC") is optional and the inclusion of a Procurement Business Number (PBN) with the proponent's proposal is optional.