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 12, 2024

Q&A 2

Q&A TABLE

No.	Proponent's Question	CMHC Response
1	Quantification Functional Requirement: Deep mathematical calculations during risk assessment. Are we expected to implement complex implementation of this nature during the first round of implementations?	No, however CMHC expects the system to have these capabilities out of the box (without any need for customization).
2	**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).** Personal Information Bank (PIB) - Is this another system being used by CMHC? Does this involve integration of PIB with ServiceNow, If yes then at what stage of the implementation roadmap would you want to leverage this system PIB. Is this system being used to bring in vendor data only?	At this point no integrations have been defined. CMHC is exploring capabilities. No integration required. The Infosource is 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 (FRENCH)
3	**Data Migration for TeamMate+** What is the volume of Historical audit project filed that need to migrate. Are there any other types of legacy data that might need migration, e.g. risk data, control data etc. Does data migration also include active data set including legacy? If legacy data is to be migrated how many years of data do we migrate and what is the file Size?	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. CMHC is only migrating an active data set (approximately 10 years of data).
4	**Control Mapping & Scoping** We would like to gain a better understanding of Financial Statements Decomposition.	The system should allow risks and controls to be associated to relevant objects, such as: Sector, Division, Process name, Process owner, Control owner, Control ID, Risks. In addition, the system should also allow for risk and controls to be associated to Financial Statement Line Items (with balances). Allowing to identify which controls are key in substantiating the Financial Statement Line Item balances. CMHC uses this to determine our annual scoping for Internal Controls over Financial Reporting (ICFR) related accounts and processes to ensure coverage with respect to materiality and key accounts and to be able to transparently disclose the coverage and impact of our annual work.

5	**Scenario analysis** We would like to gain a better understanding of what involves the Scenario analysis process.	The system should support: Maintaining a Library of Corporate Risk scenarios, organized by the impacted areas and type of scenarios (i.e. by natural disaster, cybersecurity, etc..) and prioritized by risk (potential impacts and likelihood) to CMHC. Ability to store Scenario testing results to gauge the ability to operate within tolerances for disruption across a range of severe but plausible scenarios; Ability to capture results and issues identified when conducting scenario analysis and integrate with risk profile and other risk reporting.
6	**Licensing Questions** **Risk Management:** 1. How many end users will be using the system? 2. How many risk managers/Compliance Managers or Audit Mangers would be managing the workflow? 3. How many risk/policy/compliance and audit admins are needed? 4. How many business users would be responding to the risk and compliance assessments? 5. How many auditors would be performing audit activities like control testing and etc.?	1. 200 risk & audit user licenses, including approximately: ○ Audit team - There would be 20-30 core users. ○ Users managing configurations and workflows – 5-10 ○ Other risk users (leading risk and control assessments) - 140-160 2. Business users – all employees, not concurrently to perform minimal tasks (e.g.: read and respond to tasks assigned to them, create issues and report risk event /policy violations) 3. End users – TBD

7	**General Functionality:** Ability to add attachments is available in the solution to be proposed. However, files are attached to records rather than individual fields. What is the specific use case that you would be using this capability for?	Ability to attach to records is also acceptable.
8	Do you intend to have an integration with the external system? Are you using any tool and if so, please name the tool. If not, we can perform data import manually on a defined frequency.	At this point no integrations have been defined. CMHC is exploring capabilities.
9	What integrations would you like to include in the current and future scope?	At this point no integrations have been defined. CMHC is exploring capabilities.
10	Does this mean periodic risk assessments generation? How different is this from 4.3.3 (o) and what work plan developments will be done?	The difference between items b) and o) under 4.3.3 is: - **b) Ability to track and plan periodic re-validation Scheduling (Work Plan Development).** o ability to track planned assessments for the 3 lines of defense - **0) The System should have the ability for assessment scheduling (annual, quarterly, etc.), notifications and tracking.** o ability to schedule in advance assessments and notifications to be sent automatically on a certain date as per workflows.
11	Section-H MTR-14 stipulates that **"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.**	At this point no integrations have been defined. CMHC is exploring capabilities.

	The modules to enable the selected uses cases should be fully integrated and should not require customization." However, in our review of the RFP, there are a few requirements that will require customization efforts to meet the outcomes expected by CMHC. Also, most of the requirements outlined in the RFP seems to be aiming at delivering a <u>fully matured solution</u> even in the initial phase, which in our experience is not practical and feasible to achieve without significant time and effort. Further to this, the number of integrations requested with other systems as well as risk calculation (quantification) capabilities requested are something that should be planned and achieved incrementally based on our experience as well as recommended best practices in the industry. In light of above, would you consider the following options: a. Remove / de-scope requirements that will require customization efforts on any platform (some examples of requirements that will require customization efforts are given below) b. Deliver the initial implementation scope outlined in multiple phases i.e. start with a Minimum Viable Product (MVP) both because it is our recommended / proven approach to ensure we incrementally achieve the required target state maturity and also because we do not have sufficient details in the RFP to provide an accurate pricing estimate for the full scope as listed. The MVP approach could be based on process maturity evolution i.e. simple risk assessments to quantitative to KRI based c. Provide clarity on the list of integrations and reporting / dashboarding needs required in the Phase 1 MVP	CMHC is looking for an integrated solution (without customization). Please indicate if your system has the capability out of the box or if requires customization. Once a solution is chosen, the right sequence of use cases will be selected for a phased implementation.

	d. Open to considering a multi-platform solution to meet the full scope of requirements including future state If CHMC is able to consider the options above, we would like to request for additional 4 weeks of time to provide a comprehensive response and become a strategic partner for CMHC. **Sample requirements from RFP:** **4.6.5 (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). **4.1.1 (b):** Ability to add attachments is available in the solution to be proposed. However, files are attached to records rather than individual fields. What is the specific use case that you would be using this capability for? **4.2.1:** The Proponent must respond by describing the System's quantification engine capabilities **4.1.4 (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 **4.3.7:** The Proponent must respond by describing the System's scenario analysis capabilities	

	4.3.9: The Proponent must respond by describing the System's loss and risk event capture capabilities **4.4.5:** The Proponent must respond by describing the System's budgeting, resourcing, and scheduling capabilities **4.5.1:** The Proponent must respond by describing the System's risk tracking appetite capabilities **4.6.1(b):** System should have prepopulated regulations and frameworks (NIST, ISO, etc.) **4.7.1 (c):** The System should support the Financial Statements Decomposition process (quantitative and qualitative)	
12	RFP Part 2.1.2 (A) - Mandatory Technical Requirements (page 6) states, "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." ○ Section I of Appendix C is Pre-Conditions of Award. Should this reference be revised to refer to Section H of the RFP Specifications (Appendix C) - Mandatory Technical Requirements?	Yes. This reference is to Section H. Mandatory Technical Requirements.
13	RFP Part 2.1.2 (B) - Rated Criteria (page 6) states, "CMHC will evaluate each qualified proposal based on the rated criteria as set out in Section K of the RFP Specifications (Appendix C)."	Yes. This reference is to Section J. Rated Criteria.

	○ Section K of Appendix C is Presentation. Should this reference be revised to refer to Section J of the RFP Specifications (Appendix C) - Rated Criteria?	
14	4.2.1 - How is the quantification engine intended to be used? MTR.9 references qualitative assessment criteria as opposed to a quantitative methodology. Any examples would be helpful.	See Section 4.3.3 which describes the use cases for quantification.
15	4.4 Could you confirm the number of auditors who would be utilizing the solution (core users)?	There would be 20-30 core users.
16	4.6.1g - How are risk assessments performed on regulations today? Is the regulation as a whole being risk assessed, or is it the regulation's topics/sections/individual requirements being assessed?	Compliance assessments focus on compliance with specific key provisions mapped to key controls. System needs to also have the ability to track changes to provisions and ingest data feeds from risk alert services.
17	4.7 - Are these requirements applicable to all CMHC internal controls (ICFR & GRC) or only a subset? How many tested controls are within the environment? ICFR-specific controls broken out would be great.	Yes, control requirements are applicable to all types of controls (IFCR, operational and compliance). There are approximately 400 active controls in our database currently.
18	4.9.1a - Please define "TRAs"?	Threat Risk Assessment (TRA)
19	Regarding MTR.4 would you be able to give clarity to the other applications to be integrated with, by naming the systems. 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.).	At this point no integrations have been defined. CMHC is exploring capabilities.

20	What risk alert services are to be integrated, do you currently have memberships to these services? a | The System should have the ability to ingest data feeds from risk alerts services. | 3	At this point no integrations have been defined. CMHC is exploring capabilities.
21	Does CMHC currently own/operate the ServiceNow platform? If so, can you specify the list of plugins/modules already procured and in place?	Yes, CMHC has licenses for ServiceNow Software. However, CMHC does not currently possess a license to a GRC technology.
22	How many user license counts does CMHC require for the following roles/functionality? a. **Fulfiller**: Interacts with the Workflows to complete specific daily tasks assigned to them (i.e. Perform analysis, Record risks or recommendations, Enter mitigation plans, Perform audits, etc.) b. **Business Stakeholder:** Interacts with the system only to approve plans, and review dashboards/reports. c. **Administrator:** Interacts with the system for development, system maintenance and other technical support. Moreover, require full functionality to the solution. d. **End-User/Client:** Third-party user(s) to complete intake forms or assessments or check status of existing ones.	▪ 200 risk & audit user licenses, including approximately: - Audit team - There would be 20-30 core users. - Users managing configurations and workflows – 5-10 - Other risk users (leading risk and control assessments) - 140-160 ▪ Business users – all employees, not concurrently to perform minimal tasks (e.g.: read and respond to tasks assigned to them, create issues and report risk event /policy violations) ▪ End users – TBD
23	Can CMHC share all System Architecture Diagrams (both High-Level and Low-Level), Workflow Diagrams (Flowcharts) and SOPs currently in operation and relevant to GRC solution?	Not at this time.
24	What time frame models is CMHC looking for regarding Annual and On-going Support (i.e., 24x7, 8X5, etc.)?	Section 4.1.2. - The Proponent should provide support offerings during business hours (EST hours) 8x5 and the Proponent should provide appropriate severity

		levels for support issues with clear SLAs for response and escalation process.
25	In regards to MTR 12, Section H, Appendix C, what are the hours of availability the system is expected to be 99.9% operational?	The system must be available 24x7 (99.9% of the time during hours of availability over a month).
26	In regards to R.2.11, Section J, Appendix C: a. What TeamMate+ products/services does CMHC currently utilize? b. What TeamMate+ workflows, customizations or integrations are currently in place? Moreover, if the details for each can be shared? c. What type of data currently resides within TeamMate+ and can you provide a sample dataset?	(a) CMHC utilizes Teammate+ Audit July 2023 release. (b) There are no workflows other than those setup within the TeamMate+ workflow management module. There are no customizations outside of what is allowable within the TeamMate+ Setup module. There are integrations that allow (1) to create and open MS Office and Adobe PDF files directly in TeamMate+ and (2) to receive MS Outlook email notifications from TeamMate+. (c) There is text data input directly in the system, and MS Office and Adobe PDF files attached to certain records. The data resides in MS SQL Server. There will not be sample datasets provided at this time.
27	In regards to 4.1.4, Part A, Appendix C, can you expand on data feeds and risk alert services? Can you provide a sample dataset for each data feed?	At this point no integrations have been defined. CMHC is exploring capabilities.
28	In regards to 4.1.4, Part B, Appendix C, are you looking to integrate the provided systems as part of the RFP? If so, can you provide the integration requirements for each system and associated architecture/workflow?	At this point no integrations have been defined. CMHC is exploring capabilities.

29	In regards to 4.6.1, Part C, Appendix C, what framework(s) is CMHC currently conforming to and is looking to be available within the GRC solution?	CMHC is exploring capabilities related the use of frameworks, here are some examples: NIST CSF, ISO27001:2013, COBIT, ISO 31000, etc.).
30	Due to short availability for providing detailed responses and CMHC to provide answers to pre-submission questions by Mar 1, can CHMC provide an extension to RFP submission by 2 weeks?	Refer to Amendment No 1. The new submission deadline: 21 Mar 24 2PM EST. The new deadline for Questions: 06 Mar 24.
31	Should the GRC tool be able to integrate with CMHC's Boards Management software since the Board will be reporting to the Parliament?	At this point no integrations have been defined. CMHC is exploring capabilities.
32	Will CMHC accept bids from the software vendors distributor partner?	Yes, CMHC will accept bids from authorized resellers.
33	For the Functional Requirements (R4), does the proponent have to submit its response in the table column provided?	The response must be provided in the same format.
34	To confirm, Pricing Form Table 1 - Deliverables (Initial term - 3 Years), each line item for the "Unit Cost" should be the subtotal for all 3 years, not the Annual Cost?	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).
35	Do you have any entity structure defined for assets? Do you have the following defined: - Organizational Structure - Applications with Owners and assigned to Organizational Structure	CMHC uses ServiceNow as our configuration management database according to the principles of ITIL. Configuration item records track application attributes such as infrastructure assets, approvals, etc.

	- Applications linked to devices, locations, and other assets.	We have a separate library for Organizational structure.
36	For the "200 risk and audit user licenses", do all 200 need full read and write user access? Or does a subset of them only need limited access to the entire software for oversight purposes?	▪ 200 risk & audit user licenses, including approximately: ○ Audit team - There would be 20-30 core users. ○ Users managing configurations and workflows – 5-10 ○ Other risk users (leading risk and control assessments) - 140-160 ▪ Business users – all employees, not concurrently to perform minimal tasks (e.g.: read and respond to tasks assigned to them, create issues and report risk event /policy violations) ▪ End users – TBD
37	For all the different use cases (ie: Audit, Internal Controls, Compliance, etc..), do each of those business units need their own separate environment or instance of the GRC platform? Or each of the business units doesn't mind having their data stored in the same environment as the others?	No, data can be segregated by user role access management.
38	If CMHC currently has a contract with the vendor, does the vendor still need to fill out the Vendor Information Form and Contractor Tax Forms in Schedule B?	If the selected proponent has an existing agreement with CMHC they would not be required to complete the Vendor Information Form unless updates to their information is needed.

39	Can CMHC elaborate more on the desired outcome for the following use cases: ○ Model Risk Management ○ Risk Appetite/OSRA/ERM ○ BCM ○ DRP	- Model Risk Management – see requirements under ANNEX 1 TO APPENDIX C – FUNCTIONAL REQUIREMENTS (R4) 4.11.1 - Risk appetite /ORSA/ERM - see requirements under ANNEX 1 TO APPENDIX C – FUNCTIONAL REQUIREMENTS (R4) 4.2.3 b, 4.3.1 b, 4.3.2 b, 4.3.5 a, 4.5 - BCM and DRP - see requirements under ANNEX 1 TO APPENDIX C – FUNCTIONAL REQUIREMENTS (R4) 4.10
40	Will Canada Mortgage and Housing Corporation consider exceptions and modifications to various provisions of the RFP, including its contract terms and conditions, which would be included in our proposal as exceptions? Such exceptions would include industry standard modifications such as, but not limited to, insurance items; ownership, warranty and remedy provisions typical for the type of services contemplated; indemnification obligations limited to third party claims; inclusion of a limitation of liability, etc., and be included as exceptions within our proposal.	Yes, as per Section 2.2.3 Contract Negotiation Process of the RFP "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." Any proposed "exceptions and modifications" should be included in the Proponent's bid at the time of submission to be considered to form part of its proposal.