



National Defence
National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Défense nationale
Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

**REQUEST FOR INFORMATION /
DEMANDE DE RENSEIGNEMENTS**

**RETURN RESPONSES TO /
RETOURNER LES RÉPONSES À:**

Attn:
Brittani Real
D Mar P 8-2
DMarP3BidSubmission-
DOMar3Soumissiondesoffres@forces.gc.ca

**REQUEST FOR INFORMATION
AMENDMENT/
MODIFICATION DE LA DEMANDE
DE RENSEIGNEMENTS**

Title / Titre: Risk Management Software / Logiciel pour la gestion des risques	Solicitation No / No de l'invitation: W8482-230362/A
Date 25 July/juillet 2022	Amendment No. - N° de la modification 006
Address Enquiries to – Adresser toutes questions à: Brittani Real D Mar P 8-2 DMarP3BidSubmission-DOMar3Soumissiondesoffres@forces.gc.ca	
Telephone No. / N° de téléphone: N/A	FAX No / No de fax: N/A
Destination: Specified herein	

Instructions:
See Herein.

Instructions:
Voir aux présentes

**Request for Information Closes /
La Demande de renseignements prend fin:**

At / à : 10:00 AM EDT/HAE

On / le : 10 August/août 2022

Delivery required / Livraison exigée: See Herein	Delivery offered / Livraison proposée: N/A
Vendor Name and Address / Raison sociale et adresse du fournisseur:	
Telephone No. - N° de téléphone	
Name and title of person authorized to sign on behalf of vendor (type or print) / Nom et titre de la personne autorisée à signer au nom du fournisseur (caractère d'imprimerie):	
Name / Nom: _____	Title / Titre: _____
Signature: _____	Date: _____



W8482-230362/A RISK MANAGEMENT SOFTWARE
Request for Information Amendment 006

This amendment is raised to:

- i. Provide a response to Questions 48 to 54 received from Industry.
-

1.0 Respond to Questions 48 to 54 received from Industry.

Q1: Appendix 9 in the Software Requirements Specification document is missing; namely the list of Security Controls – Could we get a copy?

A1: Appendix 9 can be provided for the RFI. An abbreviated, and bilingual, version is attached to the BuyandSell.gc.ca posting.

Q2: Annexes A, B and C in the RFI document do not provide many details of your expectations.

Q2a: Are there specific answer grids to complete or do we respond in line? What are the expectations for the response? For example, in Annex A and B do you require a Yes/No response to each requirement, or a more detailed response?

A2a: Questions in the RFI Annex E Section 3 are directly related to Annex A (Statement of Work) and Questions in the RFI Annex E Section 4 are directly related to Annex B (Software Requirements Specifications). However, there is no set expectation for the response format; Canada is agreeable to both in-line responses and answer grids. Respondents are provided latitude in formatting their response.

Regarding Annex A and B to the RFI document, the draft Statement of Work and draft Software Requirement Specifications documents are provided to illicit feedback from Potential Respondents. Should a Request for Proposal be issued for W8482-230362 – RISK MANAGEMENT SOFTWARE, responses from this RFI may be used to better develop future iterations of these documents. As such, detailed responses may be useful in developing said documentation. For example, should a respondent respond “no” to Question 3.1 in Annex E “Are there any part(s) of the scope of work defined in the Statement of Work at Annex A of this RFI that are unclear and could lead to confusion when submitting bids?”, then providing a detailed response as to which parts of the Statement of Work are unclear may help to clarify future documentation should a Request for Proposal be pursued.

Q2b: What are you looking for in Annex C – was there a document that should have been included?

A2b: Question 6.1 in the RFI Annex E Section 6 is directly related to Annex C (Financial Proposal). Canada is looking for input into the proposed methodology and breakdown to be used to evaluate potential future bids from a financial perspective.

A bilingual version of Annex C was uploaded as an Attachment to BuyandSell.gc.ca with the initial RFI. Should Potential Respondents have issues downloading/accessing

this or other documentation, Canada will supply this published documentation as required.

Q3: Is DND already leveraging a Project and Program software? (Please see sections 3.1.4 and 3.6.1). [Our software] has an offering for this, should we be discussing this, or is the expectation we will integrate with an existing solution – if so, can you provide details?

A3: Canada is not currently leveraging any Project or Program specific Software. The objective of the requirements under 3.1.4 and 3.6.1 of the Software Requirements Specification is to allow Canada to manage risks under a given project or program. This is therefore to allow access to a consolidated view of the risks under a given project or program, and equally to manage roles and access to risks under a given project and program. Those requirements are not about enabling a full range of project or program management functionalities beyond risk management.

Additionally, it is envisioned that this software will eventually be integrated with other software solutions, notably with SAP which is DND's Enterprise Resource Planning software. Requirements in section 3.4.2 of the Software Requirements Specifications discuss the need to provide an Application Programming Interface such that Canada is able to integrate the risk management solution with other software. However, the actual integration with other software (such as SAP) is currently outside the scope of this requirement.

Q4: 3.5.4 Data encryption must be achieved through the use of approved cryptographic mechanisms for protecting information up to Protected B in accordance with Ref [Q] – Could you provide more information on Ref [Q] we did not see it referenced in any of the documents?

A4: Ref [Q] is used in requirement 3.5.4 of the Software Requirements Specifications and the reference link is provided in section 1.4 of that same document. More specifically, this standard ([ITSP.40.111](#)) provides the detail of approved cryptographic algorithms that must be implemented to protect the authenticity, confidentiality, and integrity of information. Since the risk management software will handle and store information up to PROTECTED B, cryptographic algorithms within this standard must be applied. This standard provides a range of cryptographic algorithm selection such that the supplier can select which one(s) would best fit with the proposed solution.

*Q5: Can you confirm if vendors are to [(a) respond to the questions set out in “Annex E – Questions for Industry” and provide input and feedback based on the questions noted within on the RFI or (b) provide responses to Annex E **PLUS** additional components (e.g., pricing estimates for license and implementation, submitting team qualifications, etc.)].*

A5: For the purposes of this RFI, Canada is primarily seeking responses to the questions in Annex E – Questions for Industry. The purpose is to obtain industry feedback such that requirements can be amended, as required, before a potential Request for Proposal.

We certainly welcome any additional comments and feedback on the requirements documents included in Annexes A and B, or any other feedback related to this procurement effort.

- Q6: Section 3.2.1 of Annex B mentions that DND has minimum 500 simultaneous users, and 2000 users who would have access to the tool. What is the breakdown of the type of users represented by these numbers?*
- A6: Canada currently estimates the following breakdown:*
- A. Light-touch Risk & Opportunity creation/updates: around 40%*
 - B. Risk Analysis - Cost & Schedule simulations: around 10%*
 - C. Risk Management - linking related risks, roll-ups, monitoring & oversight: around 10%*
 - D. Read-only monitoring: around 40%*
- Q7: Approximately how many existing risks would be imported into the solution and from what source(s)?*
- A7: Para 3.2.7.1 of the Statement of Work asks for support to migrate the current risks from the Airworthiness Risk Management Information System. This Microsoft Access tool, supported by an SQL database, has a total of 60 active RARM (Record of Airworthiness Risk Management) currently being managed by Weapon System Managers. The total number of records in the DGAEPM database is about 2,600. The import of other risks beyond airworthiness would not be within the scope of this procurement and would be done manually by Canada once the solution is operational.*
- Q8: Section 3.4.2 of Annex B mentions an Application Programming Interface (API). Please describe the integrations with other applications/systems that are required / potentially desired. Is DND primarily interested in including ARM data in another application, or using other applications to modify or interact with ARM?*
- A8: Actual integration between the risk management software and other applications is currently out of scope due to a number of other ongoing projects that are necessary to enable such integration. The goal will be to enable communication both ways such that risks can be imported from notifications in our Enterprise Resources Management system (SAP based) and exported to other solutions. As such, the objective of asking for the Application Programming Interface is to get a generic set of functions (web services for instance) that we can call up to integrate with other applications.*
- Q8a: Are the future potential interconnected applications deployed internally within DND-managed information systems and are they COTS?*
- A8a: They would be deployed within DND-managed information systems, and are for the most part COTS.*
- Q8b: Are there other tools in mind to integrate that you would want to specify?*
- A8b: Currently, we are looking to keep the API as generic as possible to allow for flexibility in any future integration.*

Q9: Is DND entertaining a range of solutions for this need? Is there a preference between commercial-off-the shelf (COTS) vs. custom solutions?

A9: At this stage, we are leaving it for industry to propose a best value for money solution. This must take into consideration the balance between implementation cost and sustainment cost. As such, COTS will always be much preferred such that we can leverage existing solutions which are generally more cost effective to procure, deploy, and sustain in the long term (patching, maintenance). It is however envisioned that our requirements may require a mix of more than one COTS software (notably to perform workflows).

Q10: Section 2.3 of the main RFI document mentions a Request for Proposal will follow in September 2022 with contract award in December 2022. Please provide additional details about what this process will entail? For example, will there be scheduled product demonstrations prior to Request for Proposal? Any shortlisting of potential vendors?

A10: Per Section 1.1.3, this RFI “is not to be considered as a commitment to issue a subsequent solicitation” hence it is key to note that Section 2.3 represents the anticipated Request for Proposal timeline should Canada proceed to that stage. The Request for Proposal process, and more specifically the bid evaluation plan, has yet to be fully determined. Part of it will depend on feedback received from industry during the RFI process. Any input on how to best proceed with a goal to obtain a best value for money solution through a fair and objective procurement is most welcome. At the moment, there is no intent to shortlist potential vendors, however we are considering on including a demonstration portion during the bid evaluation process. This demonstration would serve to assess the user experience of the proposed solutions against a pre-determined set of key risk management functions defined in the Software Requirements Specifications. It is expected that all solutions would require a level of configuration to fully meet Canada’s requirements. These demonstrations as part of the bid evaluation would likely focus on high level common risk management functions that would be expected from a COTS solution. They may also serve to assess the maturity of the proposed solution to keep the developmental risk to a minimum and align to existing COTS as much as possible.

Q11: The RFI contains references to content that is hosted on DND intranet sites (i.e – page 34 of Annex B). If this information also forms part of the RFI requirements, can this information be provided directly?

A11: Yes, it can. If some documentation is required in order to provide better feedback during the RFI, then Canada can provide the references. All of the references will be made available should Canada proceed with a Request for Proposal.

Q11a: Should we put a list together of the documents we think would help us in developing our response?

A11a: Respondents can request references found on DND intranet sites by submitting their request to the RFI contact e-mail, and the Contracting Authority can provide the requested documents.

Q12: Please explain what is meant by “default risk” as opposed to the specific risk domains listed in Appendix 4 of Annex B?

A12: The default risks set the foundation for what minimum information is required to raise a risk or opportunity without raising a risk using one of the specific risk domains. It is not expected that this type would be widely used, however it does provide the opportunity for a user to raise a basic risk even if they are not sure which specific domain to use. Ideally, the risk management software solution would simply allow Canada to simply create and personalize different types of risks and opportunities.

Q13: Does DND have a target date for the implementation / go-live for the solution?

A13: At the moment we do not. It is expected that this will be determined collaboratively through the development of the deliverable PM-001 Project Schedule. Evidently, as this solution is intended to be deployed in a DND-managed cloud environment (a subscription on Microsoft Azure), a number of steps do rely on Canada's input. We listed those key activities and milestones in the Data Item Description of deliverable PM-001 which would drive the overall schedule and eventual go-live milestone.

Q14: Will issue and incident tracking form part of this requirement?

A14: Currently issue and incident tracking do not form part of our mandatory scope but is something we may consider as an asset.

Q15: What is the feedback process after submitting the RFI?

A15: Currently DND does not have plans to further engage with industry. Our intentions remain aligned with the proposed schedule in section 2.3 of the RFI, however follow-on RFIs (including draft Request for Proposal(s)) may be issued.

Q16: What value would you like to have out of having all the risk domain areas in one database versus multiple dedicated spaces?

A16: The objective is to be able to generate a list of risks associated with a given project, program, or platform (for example) regardless of their domain. For example, a project can have security risks, project risks, and ammunition and explosive risks. This would allow the project to manage their consolidated risks and assess their aggregate risk level based on all types of risks. The data associated with the different risk domain areas can be stored in separate databases in the background.

Q17: Is there a need to track Segregation of Duties Compliance between the authorized roles?

A17: Yes. We do need segregation of duties and controls over authorized roles. As such, tracking is required. This is part of a few key security controls that need to be implemented as part of the Security Assessment & Authorization process.

Q18: How is the DND managing the risks in the RFI and other business risks today?

A18: Project and Program risks and opportunities: Policies are defined and referenced in the Software Requirements Specifications. There are no specific processes and no mandated tools. Capital Projects will report on high-level risks at senior boards via the Project System module within DND's Enterprise Resource Planning tool. However, the day-to-day risk management and analysis is done ad-hoc by the project team via excel spreadsheets,

SharePoint, or it is being contracted out to industry to manage. Opportunities are rarely tracked.

- *Security Risk and Cyber Security: Policies are defined and referenced in the Software Requirements Specifications. There are no specific processes and no mandated tools. Similar to project and program risks, they are generally tracked ad-hoc via excel spreadsheets.*
- *Ammunition and Explosive Safety Risks: A policy and process exists for this, however there are no mandated tools. Ultimately, those risks are captured in Word documents which are submitted for review and approval.*
- *In-Service Naval Materiel Risks: Policies, Processes, and mandated tools exist for this, however the current method and tool is not the most efficient and does not allow for efficient management of risk. Those risks start off as a Risk Management Record (Word document) being reviewed, and then the information from that document is copy/pasted into a Notification via the Plant Maintenance module within SAP. This notification is then submitted for review (through status change) through the stakeholders. The official approval/endorsement is done via the release of a military message from the Operational Authority. That message is then copy/pasted into the Notification within SAP.*
- *Airworthiness Risks: Policies, Processes, and mandated tools exist for this. The process typically starts with email notifications and is followed by the tracking of risks using the current Microsoft Access tool supported by an SQL database. Not every aspect is done via the Microsoft Access tool, and therefore Word documents are still used where required. The airworthiness risk management process begins with risk identification. When risk is identified, an Airworthiness Impact Assessment is performed to determine the risk level index. If the risk level index is above the Acceptable Level of Safety (ALOS) then a Risk Alert Notification (RAN) is issued to all stakeholders (email). The RAN is then acknowledged by appropriate authority. Within 24 hrs from the time the RAN was issued, an Airworthiness Risk Alert (ARA) is drafted and issued. The purpose of the ARA is to advise all stakeholders, of the situation (risk & level of confidence), the steps taken to fully determine the actual risk level, and any mitigating actions planned or in place as interim measures. The final step is the Record of Airworthiness Risk Management (RARM) being drafted to capture (within 14 days following the ARA), identify and manage airworthiness risk issues including mitigating activities. ARA and RARM are formally documented in the MS Access Database and the database is also used to track mitigating activities. Signed copies of risk assessments (ARA and RARM) are saved in a different repository. If the risk is not approved, there has to be a new version of the RARM that must be issued, which is an airworthiness requirement. Additionally, an action plan must be tracked for risk mitigation strategy to follow through on deadlines.*

Q19: What risk management framework do you use today?

A19: The overarching risk management framework is the one developed by Treasury Board: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=19422>. This framework provides guidance to deputy heads on how to implement effective risk management practices at all levels of their organization.

Q20: How do you handle enterprise risk reporting today?

A20: The enterprise risk reporting is mostly done via DND's Enterprise Resource Planning tool at a higher level. However, the aim of this risk management software is to allow for better management of risks at the tactical level, and thus increase our strategic understanding of the risk level. It is not meant to conduct risk reporting at the enterprise (DND) level although the data will evidently influence such reporting.

Q20a: Will simulations form part of the requirement?

A20a: No, there are no specific requirements for simulations.

Q21: What is the volume of risks you are planning to manage?

A21: As there is currently no single solution to effectively manage risks, this number is hard to determine. This number will also vastly vary based on the level of adoption by various organizations and projects. The current airworthiness risk database has a total of 2,600 items. There will be an estimated 200 active Naval Materiel Risks, 50 active Security and Cyber Security risks, 20 active ammunition and explosive safety risks, and 2,000 active project and program management risks and opportunities.

Q22: What are the business areas of risk you are planning to address, besides the ones mentioned in the RFI?

A22: None beyond what is mentioned in the RFI. It is expected that as Canada matures their way to conduct risk management, future capabilities or changes would be required. Under this procurement, there would be provision for emergent tasks to address those gaps.

Q23: How often do you perform risk assessments? Is it done annually, or as needed?

A23: It depends on the type of risk. Typically, most projects with good risk management practices will conduct risk assessment at least once a month (depending on the project complexity). Security and Cybersecurity risks are performed routinely (schedule depends on the system's confidentiality, integrity and availability risk profile) and as needed when a vulnerability is identified. Naval Materiel risk management are raised and assessed as needed (once a new risk is identified). Airworthiness Risks are assessed as needed once a new risk is identified for each fleet. On average, about 20-30 new risk assessments are generated and recorded in the current tool (MS Access database) every year. Routinely throughout their lifecycle, risk assessments are updated/revised to capture new information as needed. Q21: How many objects/assets do they want to track?

A24: The Software Requirements Specifications includes a list of all aircraft fleets and classes of ships against which Canada wants to be able to assess risks. Furthermore, the requirements also include the need to track risks at the equipment level with pre-determined lists. Additionally, it is expected that the software would be required to track hundreds of projects and programs against which risks would be raised.

Q24A: Do you have a hierarchy of aircrafts and vessels? For example, are risks tracked down to the equipment/materiel hierarchy, or is risk tracked at the asset/project level?

- A24A: We have a requirement to have the ability to track risks at the fleet/class level, individual platform/aircraft level, and equipment level. The lists for each of these levels are included in the Software Requirements Specifications.*
- Q25: We expect that you will be working with a System Integrator, and the software vendor will be providing design guidance and participation throughout the project. Are you also looking for a managed services?*
- A25: Since this software is not intended to be integrated beyond the necessary integration within the cloud environment (for authentication and SMTP for example), we do not intend on having a separate System Integrator. The tasks identified within section 3.2 of the Statement of Work are meant to support DND in performing the full range of functions required to deploy and configure the risk management software within the DND-managed cloud environment (Microsoft Azure subscription).*
- Q26: The risk management solution is expected to integrate with other software solutions (such as SAP). What other software solutions may eventually be integrated into the risk management solution?*
- A26: The actual integration with external solutions is currently out of scope. Yes, it is expected that one day integration will be made with the DND Enterprise Resources Planning software, which is SAP-based. We also envision that the risk management software will integrate with other tools that are being, or will be, deployed in the greater cloud-based Integrated Data Environment.*
- Q26A: Are you expecting the contractor to do all the configuration work in your environment, or would the contractor be working alongside DND to complete this work?*
- A26A: The expectation is for the Contractor to perform the deployment and configuration of the solution in the DND-managed cloud subscription during the implementation phase. In order to do so, DND will provide the contractor with privileged access to the subscription. DND will be involved in monitoring and supporting the work as required.*
- Q27: What is the classification of the data, both individual data elements and data in aggregate?*
- A27: Section 3.7.3 of the Software Requirements Specifications discusses security requirements. Individual elements can be up to Protected B. It is not expected that the aggregation of the data will lead to a classification above Protected B.*
- Q28: What is the security classification of source systems that are potentially integrating with the risk management solution?*
- A28: The source systems will be at most Protected B (our SAP-based Enterprise Resource Planning system).*
- Q29: In the context of in-service support-like contracts, is the system expected to interface in any way with industry solutions?*
- A29: At the moment it is not. The idea is to deploy this solution into our DND-managed cloud environment and provide access to industry on a need basis. The risk management solution,*

and its data, would therefore be entirely managed and owned by DND. This procurement is a step towards a greater Integrated Data Environment where DND will be managing integrated solutions and data, and provide access to industry to collaborate on programs and projects using the same set of tools and data. This includes, but is not limited to, collaboration via the various in-service support contracts.

Q30: How many users will be accessing the system?

A30: As per paragraph 3.2.1 of the Software Requirements Specifications, we ask for a minimum of 500 simultaneous users, and a minimum of 2000 users with access to the application. As we currently do not have a common solution to properly manage risk in all of the domains mention in the requirements, these numbers are hard to assess.

Q31: Are you looking for a managed service model where the vendor provides all aspects from deploying cloud infrastructure, supporting upgrading, managing, and configuring the application, or is there an on-premises Cloud permutation that you are looking for, from a deployment perspective?

A31: The vision is that this procurement is to ultimately obtain software that will be deployed on-premises (within the cloud subscription managed by DND). The contractor would be given access to this cloud subscription in order to deploy and configure the solution. Once it is operational, it would be turned over to DND to be managed through its lifecycle. It is expected that an annual maintenance fee would be paid by DND in order to gain access to future software releases and for the contractor to address technical issues as stipulated in standard SACC clauses.

Q31a: Once you're live, would DND be responsible for the care and management of the software, or would this be contracted out as part of the service model?

A31a: At the moment, the object is that once live DND would be responsible for the management of the software. DND would require access to future release and updates to the software, however DND would be responsible for the configuration management of the solution within the DND-managed cloud environment and deploy those future releases and updates. If there is a requirement for additional functionality, this may be done through emergent tasks on the contract.

Q31b: Have you considered a managed services model?

A31b: Yes, it has been considered. The goal is to minimize costs for DND and taxpayers, and migrate all services into one service desk, where DND would manage all software deployed within the spoke. This service desk and IT support organization is already being stood up under other projects.

Q31c: Would the procurement consider a Software-as-a-Service (SaaS) instead of an on-premise solution?

A31c: Currently, DND would consider a SaaS, however the current requirements are for the procurement of an on-premise solution for several reasons. An on-premise solution:

- *ensures complete and unique control over the data (both in transit and at rest), especially as it will contain Controlled Goods and data up to Protected B;*

- *allows for easy integration with the Active Directory managed centrally and used by other similar applications;*
- *allows for easy integration with other applications collocated in the same subscription both from an API perspective and a database access perspective, and that without having to expose data outside the DND-managed subscription;*
- *allows to manage Role-Based Access Control centrally using roles that can assign pre-determined access to users for a number of applications;*
- *reduces the IT security risks associated with the constant transfer of data outside the subscription (through the internet)*
- *reduces duplication of cost associated with security monitoring, and other administrative functions that already have to be provided by DND for other applications deployed in the same subscription.*

Therefore, it is not to say that a SaaS solution couldn't meet the above aspects, however there are inherently a number of risks that come with this approach. If this were a one-of procurement with no intention to further integrate the solution with any other applications, then we would likely be undergoing a SaaS approach instead of on-premise.

Q32: The requirements speak to Microsoft Azure specifically, is there a reason that other public cloud providers wouldn't be considered?

A32: Although the Government of Canada can put in place contracts with all major public cloud providers (Google, Amazon Web Series, Microsoft Azure), a Microsoft Azure subscription is already in place where other projects are currently being deployed and are targets for integration with the risk management software. As such, in order to reduce complexity and reduce IT security risks associated with data transfer between subscriptions, the goal is to deploy the risk management software within the existing Azure subscription.

Q33: What is the budget for this procurement?

A33: The budget will depend on feedback from industry through one of the key question of Annex E. This question from Annex E is important for DND in order to seek appropriate funding before launching the Request for Proposal. This procurement is not intended to be a capital project (valued above \$4.5M). Considering the current requirements, the goal to leverage COTS as much as possible, and the fact that integration with other solutions is out of scope, Canada is expecting that the budget required for this procurement would be well below the \$4.5M threshold. The overall budget must also take into considering the implementation, licenses, and sustainment of the solution as this is all part of the overall contract value. Those aspects will all be calculated, as seen in the draft Financial Proposal (Annex C) document which has been provided with the RFI.

Q33a: Will the type of funding (capital vs maintenance) be affected by the subscription model?

A33a: Yes, there is some expected impact. Initial implementation work along with lifetime licenses are procured using capital funding. Maintenance and recurring licenses are

procured using maintenance funding. Although Canada's preference is to obtain lifetime licenses for an unlimited number of user (which makes it easier for wide adoption, and likely good value for money in the long term) both model are currently offered in the draft Financial Proposal (Annex C).

Q34: Why isn't the risk management capability procured as part of the Defence X (DRMIS modernization) project?

A34: The scope that the Defence X project (DRMIS Modernization) will deliver is still being determined, therefore we are uncertain if a Risk Management capability that meets our requirements will be delivered as part of this project. The intent of this risk management software procurement will be to have an initial contract period that covers for the gap until Defence X is implemented, and then option years to extend the capability to account for a transition period and potential delays.

Q35: The provisions of SACC Clause 4002 (Software Development or Modification Services) are not aligned with the nature of a SaaS application. What is the basis of the coding related requirements in SACC Clause 4002 and can the desired effect can be achieved through software that has been effectively designed to enable client configuration?

A35: As per A31c, the vision is that this procurement is to ultimately obtain a software that will be deployed on-premise (within the cloud subscription managed by DND). The contractor would be given access to this cloud subscription in order to deploy and configure the solution. Once it is operational, it would be turned over to DND to be managed through its lifecycle. It is expected that an annual maintenance fee would be paid by DND in order to gain access to future software releases and for the contractor to address technical issues as stipulated in standard SACC clauses.

Despite the on-premise deployment approach, it is DND's intention to minimize as much as possible any customization of the application (code changes) unless absolutely necessary. The idea would be to procure a solution that does allow for flexibility through configuration available within the application. This approach will ensure that DND is able to upgrade to future releases of the application as they become available with ease.

Q36: Have you considered stating requirements around data and database such that Canada can easily extract the data and import it into a new software solution should you decide to change software provider along the way?

A36: Yes. Para 3.7.5.1.1 of the Software Requirements Specifications states that "the data generated by the risk management software must not be dependent on the use of a specific commercial proprietary application." This is to allow Canada full and complete access to its data at any time, regardless of the application used to perform risk management.

Q37: How could we (as a software vendor) be accountable for software issues if Canada has the ability to modify the software code?

A37: Canada does not intend on modifying the code of the software. It is our intention to clearly state that the contract clauses about code modification are applicable for the custom deployment scripts that have to be developed as part of this contract where the IP would belong to Canada.

Q38: How would we (as software vendor) ensure that our IP is protected if we allow Canada to modify the code, which would require full access to the IP associated with the software?

A38: It is Canada's intention to respect the IP that belongs to a software vendor, especially as it pertains to the core risk management software. However, the IP for any custom scripts or code that would be developed as part of this contract would belong to Canada.

Q39: How do you intend on applying the quality management clauses that allow for the overseeing of code development?

A39: It is not Canada's intention to oversee the vendor develop and code that pertains to the core risk management software. SACC Manual clause 4002 is meant to provide the ability to oversee the development of custom scripts or code that would be develop as part of this contract, and to oversee the deployment and testing of the software within the DND-managed cloud environment.

Q40: We note that Canada requires the software vendor to discharge the project management function for implementation of the software solution and anticipates that Canada will be seeking to project manage the associated process changes within MEPM and AEPM. What would be the contractor's ability to task and manage the DND human resources across the various stakeholder departments required for project delivery?

A40: Canada does not intend on discharging all project management functions to the contractor. Canada will remain the prime project manager for this project. However, due to shortages of staff, Canada does ask the contractor to perform several key functions that will help DND in managing the project and reduce execution risk. Those functions, and associated deliverables, are listed in the Statement of Work.

The Contractor would not have the authority to task human resources across various stakeholders' departments. DND will provide access to key resources to support the contractor and the established timeline as much as possible, within the constraints and priorities of each department.

Q40a: Would the contractor have access to Canada's IT system?

A40a: The Contractor will be given privileged access to the DND-managed cloud subscription in order to perform the tasks from the Statement of Work (notably to deploy and configure the risk management solution).

Q40b: How will Canada approach potential Conflict of Interest (ex: regarding benefits realization)?

A40b: As Canada will remain the overall project manager for the execution of this project, we do not see any potential conflict of interest.

Q41: Is Canada interested in understanding the wider scope of capability from potential vendors, and would Canada wish to apply weighting to that scope?

A41: As part of this RFI Canada welcomes any suggestion of additional functionalities that we should consider including as part of our Software Requirements Specifications in order to better perform risk management. Those can be provided via the response to the RFI.

However, Canada cannot attribute weight to capabilities that could meet potential requirements not in scope of the procurement (beyond the existing mandatory and desirable requirements).

It is Canada's intention that any resulting contract would allow for the provision of emergent tasks such that any new requirements (such as new capabilities) can be addressed along the way. It is expected that there are several unknown functionalities that Canada may require in the future as we continue to mature some of the policies and business processes around risk management. When those functionalities become known, then emergent tasks may be raised for the contractor to develop a solution that meet the need.

Q42: Is DND looking for COTS solution?

A42: Yes, DND is looking for COTS in order to minimize the risk, minimize the implementation and lifecycle cost, and reduce the implementation timeline as much as possible.

Q43: Has DND considered all relevant government standards?

A43: Yes, DND has considered key government standards, as included in our Software Requirements Specifications. Beyond IT security related standards, these standards include those related to accessibility, usability, and official languages.

Q44: Can DND explain further the premise of hub and spoke?

A44: Details on the concept of landing zone (or tenant, or hub) can be accessed via the Microsoft website: <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/>

Within the context of the Joint Defense Cloud Program, a common DND enterprise landing zone (referred to as the tenant, or the hub) is centrally available for all DND-managed subscriptions (or spoke). This approach allows for several common services to be provided from the hub to the different spoke (services such as Active Directory, and SMTP) as well as to provide the baseline security to manage external facing data exchange (both to the internet and to the on-premise network). By deploying the risk management software within one of the spoke, we are also inheriting a high number of security controls implemented by the hub leaving around 58 controls to be implemented by the spoke and applications deployed within the spoke. This approach therefore allows to reduce cost, and IT Security risks.

Q45: How does DND plan to achieve a one-month Authority to Operate (ATO)?

A45: This can be achieved via the fact that the risk management software would be deployed in a spoke environment within a cloud tenant (or hub) where a high number of security controls would already be inherited by the tenant (or hub). Additionally, a number of parallel projects are ongoing to mature this environment such that it can reach an ATO for Protected B. Those would contribute to a shortened ATO associated with the risk management software.

Q46: Will the RFP be accepting bids from only software vendors themselves or resellers as well?

A46: Should Canada proceed to RFP stage, the intention would be to accept bids from Software Publishers as Bidder or from Resellers as Bidders. The bid recommended for contract award

could potentially be a partnership where a supplier will perform the work and deliver a third-party software from which they obtained the rights to sell to Canada from the Software Vendor company.

Q47: *What is the timeline for the RFP?*

A47: *As per the RFI, should a follow-on RFP be issued, the current objective is to launch the RFP between mid to end of September, such that the bid evaluation can be conducted in November, and a contract awarded in December. Evidently, there are several factors that could extend this timeline, but this is the current objective the team is working towards.*

Q48: Is financial risk management (i.e. procurement vetting/screening) included in the scope of this RFI?

A48: Project and Program risks can be directly linked to budget / finance. Those can include risks associated with procurement efforts to support the associated project or program.

Q49: How does supplier risk and assessing the risks associated with third parties factor into this request? (e.g. regulatory & reputational risk, sanction screening, negative news monitoring, adverse foreign exposure, etc.)

A49: As per A48, risks associated with procurement efforts for a project or program would fall under Project and Program risks.

Q50: Is there a need to understand the beneficial owners, key persons of control, and ownership structures of suppliers/contractors?

A50: No, there is no need beyond what would be required to be provided to support the Government of Canada Security Clearance process.

Q51: Are Climate risk data and analytics included in the scope of this RFI?

A51: No, they are not.

Q52: If a combined set of risks identified in this RFI go beyond the specific solutions of our company, will the Government consider a combined response with our trusted partners offering a modular approach?

A52: Refer to A46.

Canada would prefer to have one license agreement from the Reseller, even if more than one third-party vendor may be involved in providing the solution.

Q53: Can the Government provide a list of examples of risk/issues that it is seeking to prevent with a potential tender?

A53: The objective of this procurement is to obtain a risk management software such that DND can raise, track, and manage risk at a tactical level. This will in turn inform decision making at the strategic and enterprise level. This software will be used to help DND better manage the various types of risks in support of business processes under the materiel acquisition and support umbrella.

Q54: We consider many of our capabilities to be unique. Will the Government consider any of the specific requirements under sole source authorization?

A54: No, Canada will not be considering requirements for sole sourcing as part of this requirement. Any additional requirements that respondents believe should be added as part of the Software Requirements Specification or Statement of Work should be submitted to Canada via the response to the RFI such that it can be considered.

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED.