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

Title / Titre:	Solicitation No / No de l'invitation:
Risk Management Software / Logiciel pour la gestion des risques	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	

REQUEST FOR INFORMATION AMENDMENT/
MODIFICATION DE LA DEMANDE DE RENSEIGNEMENTS

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:	Delivery offered / Livraison proposée:
See Herein	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:** _____	

Canada

W8482-230362/A LOGICIEL POUR LA GESTION DES RISQUES

Modification de la Demande de renseignements 006

Cette modification est soulevée pour :

i. Offrir une réponse aux questions 48 à 54 reçues de l'industrie.

1.0 Répondre aux questions 48 à 54 reçues de l'industrie

Q1: L'annexe 9 du document de spécification des exigences logicielles est manquante, à savoir la liste des contrôles de sécurité - Pourrions-nous en obtenir une copie ?

A1: L'annexe 9 peut être fournie pour la DDR. Une version abrégée, et bilingue, est jointe à l'affichage de BuyandSell.gc.ca.

Q2: Les annexes A, B et C du document de demande d'informations ne fournissent pas beaucoup de détails sur vos attentes.

Q2a: Y a-t-il des grilles de réponses spécifiques à remplir ou devons-nous répondre en ligne ? Quelles sont les attentes en matière de réponse ? Par exemple, dans les annexes A et B, avez-vous besoin d'une réponse Oui/Non à chaque exigence, ou d'une réponse plus détaillée ?

A2a: Les questions de la section 3 de l'annexe E de la DDR sont directement liées à l'annexe A (énoncé des travaux) et les questions de la section 4 de l'annexe E de la DDR sont directement liées à l'annexe B (spécifications des exigences logicielles). Toutefois, il n'y a pas d'attente précise quant au format des réponses ; le Canada accepte les réponses en ligne et les grilles de réponses. Les répondants ont toute latitude pour formater leur réponse.

En ce qui concerne les annexes A et B de la demande de renseignements, l'ébauche de l'énoncé des travaux et l'ébauche des spécifications des exigences logicielles sont fournies afin de recueillir les commentaires des soumissionnaires potentiels. Si une demande de proposition est émise pour W8482-230362 - LOGICIEL POUR LA GESTION DES RISQUES, les réponses à cette DDR peuvent être utilisées pour mieux développer les itérations futures de ces documents. À ce titre, des réponses détaillées peuvent être utiles pour développer lesdits documents. Par exemple, si un répondant répond "non" à la question 3.1 de l'annexe E "Y a-t-il une ou plusieurs parties de l'étendue des travaux définie dans l'énoncé des travaux à l'annexe A de la présente DDR qui ne sont pas claires et qui pourraient prêter à confusion lors de la soumission des offres ?", alors le fait de fournir une réponse détaillée quant aux parties de l'énoncé des travaux qui ne sont pas claires pourrait aider à clarifier la documentation future si une demande de proposition était lancée.

Q2b: Que cherchez-vous dans l'annexe C - y a-t-il un document qui aurait dû être inclus ?

A2b: La question 6.1 de la section 6 de l'annexe E de la DDR est directement liée à l'annexe C (proposition financière). Le Canada souhaite obtenir des commentaires sur la méthodologie et la structure proposées qui seront utilisées pour évaluer les futures offres potentielles d'un point de vue financier.

Une version bilingue de l'annexe C a été téléchargée en tant que pièce jointe sur le site BuyandSell.gc.ca avec la DDR initiale. Si les soumissionnaires potentiels ont des difficultés à télécharger/accéder à cette documentation ou à d'autres documents, le Canada fournira cette documentation publiée au besoin.

Q3: Le MDN utilise-t-il déjà un logiciel de projet et de programme ? (Veuillez consulter les sections 3.1.4 et 3.6.1). [Notre logiciel] a une offre à cet égard, devrions-nous en discuter ou nous attendons-nous à ce que nous nous intégrions à une solution existante - si oui, pouvez-vous fournir des détails ?

A3: Le Canada n'exploite actuellement aucun logiciel propre à un projet ou à un programme. L'objectif des exigences des sections 3.1.4 et 3.6.1 de la spécification des exigences logicielles est de permettre au Canada de gérer les risques liés à un projet ou à un programme donné. Il s'agit donc de permettre l'accès à une vue consolidée des risques d'un projet ou d'un programme donné, et également de gérer les rôles et l'accès aux risques d'un projet ou d'un programme donné. Ces exigences ne visent pas à permettre une gamme complète de fonctionnalités de gestion de projet ou de programme au-delà de la gestion des risques.

De plus, il est prévu que ce logiciel sera éventuellement intégré à d'autres solutions logicielles, notamment à SAP qui est le logiciel de planification des ressources d'entreprise du MDN. Les exigences de la section 3.4.2 des spécifications des exigences logicielles traitent de la nécessité de fournir une interface de programmation d'applications de sorte que le Canada puisse intégrer la solution de gestion des risques à d'autres logiciels. Cependant, l'intégration réelle avec d'autres logiciels (comme SAP) est actuellement en dehors de la portée de cette exigence.

Q4: 3.5.4 Le cryptage des données doit être réalisé par l'utilisation de mécanismes cryptographiques approuvés pour protéger les informations jusqu'au niveau Protégé B conformément à la Réf [Q] - Pourriez-vous fournir plus d'informations sur la Réf [Q], nous n'avons pas vu qu'elle était référencée dans aucun des documents ?

A4: La référence [Q] est utilisée dans l'exigence 3.5.4 du Spécifications des exigences logicielles et le lien de référence est fourni dans la section 1.4 de ce même document. Plus précisément, cette norme (ITSP.40.111) fournit le détail des algorithmes cryptographiques approuvés qui doivent être mis en œuvre pour protéger l'authenticité, la confidentialité et l'intégrité des informations. Étant donné que le logiciel de gestion des risques traitera et stockera des informations jusqu'au niveau PROTÉGÉ B, les algorithmes cryptographiques de cette norme doivent être appliqués. Cette norme fournit une gamme de sélection d'algorithmes cryptographiques de sorte que le fournisseur peut choisir celui ou ceux qui s'adapteraient le mieux à la solution proposée.

Q5: Pouvez-vous confirmer si les fournisseurs doivent [(a) répondre aux questions énoncées dans « l'Annexe E - Questions pour l'industrie » et fournir des informations et des commentaires sur la base des questions mentionnées dans la DDR ou (b) fournir des réponses à l'Annexe E ***AINSI QUE*** *des éléments supplémentaires (par exemple, des estimations de prix pour la licence et la mise en œuvre, soumettre les qualifications de l'équipe, etc.]*

A5: Aux fins de la présente DDR, le Canada cherche principalement à obtenir des réponses aux questions de l'annexe E - Questions pour l'industrie. Le but est d'obtenir les commentaires de

l'industrie afin que les exigences puissent être modifiées, au besoin, avant une demande de proposition potentielle.

Nous accueillerons volontiers tout commentaire supplémentaire et toute rétroaction sur les documents relatifs aux exigences inclus dans les annexes A et B, ou toute autre rétroaction relative à cet effort d'approvisionnement.

Q6 : La section 3.2.1 de l'annexe B mentionne que le MDN a un minimum de 500 utilisateurs simultanés, et 2000 utilisateurs qui auraient accès à l'outil. Quelle est la ventilation du type d'utilisateurs représentés par ces chiffres ?

A6 : Le Canada estime actuellement la répartition suivante :

A. Création/mise à jour de risques et d'opportunités : environ 40 %.

B. Analyse des risques - simulations de coûts et de délais : environ 10 %.

C. Gestion des risques - mise en relation des risques liés à l'activité, récapitulations, suivi et surveillance : environ 10 %.

D. Surveillance en lecture seule : environ 40%.

Q7 : Environ combien de risques existants seraient importés dans la solution et de quelle(s) source(s) ?

R7 : Le paragraphe 3.2.7.1 de l'énoncé des travaux demande un soutien pour la migration des risques du système d'information sur la gestion des risques de navigabilité. Cet outil Microsoft Access, soutenu par une base de données SQL, compte un total de 60 RARM (Record of Airworthiness Risk Management) actifs actuellement gérés par les gestionnaires de systèmes d'armes. Le nombre total d'enregistrements dans la base de données DGAEPM est d'environ 2 600. L'importation de risques autres que la navigabilité n'entre pas dans le cadre de ce contrat et sera effectuée manuellement par le Canada une fois que la solution sera opérationnelle.

Q8 : La section 3.4.2 de l'annexe B mentionne une interface de programmation d'applications (API). Veuillez décrire les intégrations avec d'autres applications/systèmes qui sont requises / potentiellement souhaitées. Le MDN est-il principalement intéressé à inclure les données du MRA dans une autre application, ou à utiliser d'autres applications pour modifier ou interagir avec le MRA ?

R8 : L'intégration réelle entre le logiciel de gestion des risques et d'autres applications est actuellement hors de portée en raison d'un certain nombre d'autres projets en cours qui sont nécessaires pour permettre une telle intégration. L'objectif sera de permettre la

communication dans les deux sens, de sorte que les risques puissent être importés à partir de notifications dans notre système de gestion des ressources de l'entreprise (basé sur SAP) et exportés vers d'autres solutions. En tant que tel, l'objectif de la demande d'interface de programmation d'applications est d'obtenir un ensemble générique de fonctions (services Web, par exemple) que nous pouvons appeler pour les intégrer à d'autres applications.

Q8a : Les futures applications interconnectées potentielles sont-elles déployées à l'interne dans les systèmes d'information gérés par le MDN et sont-elles disponibles commercialement ?

R8a : Elles seraient déployées dans les systèmes d'information gérés par le MDN et sont pour la plupart des applications commerciales.

Q8b : Avez-vous en tête d'autres outils à intégrer que vous voudriez préciser ?

R8b : Actuellement, nous cherchons à garder l'API aussi générique que possible pour permettre une certaine souplesse dans toute intégration future.

Q9 : Le MDN envisage-t-il une gamme de solutions pour répondre à ce besoin ? Y a-t-il une préférence entre les solutions commerciales et les solutions personnalisées ? R9 : À ce stade, nous laissons à l'industrie le soin de proposer une solution offrant le meilleur rapport qualité-prix. Cette solution doit tenir compte de l'équilibre entre le coût de mise en œuvre et le coût de maintenance. En tant que telle, les solutions commerciales seront toujours préférées car elles permettent d'exploiter des solutions existantes qui sont généralement plus rentables à l'achat, au déploiement et au maintien à long terme (correctifs, maintenance). Il est cependant envisagé que nos besoins puissent nécessiter une combinaison de plus d'un logiciel commercial (notamment pour exécuter des flux de travail).

Q10 : La section 2.3 du document principal de la DDR mentionne qu'un appel d'offres sera lancé en septembre 2022 et que le contrat sera attribué en décembre 2022. Pourriez-vous fournir des détails supplémentaires sur ce que ce processus impliquerait ? Par exemple, y aura-t-il des démonstrations de produits prévues avant l'appel d'offres ? Y aura-t-il une présélection des fournisseurs potentiels ?

R10 : Conformément à la section 1.1.3, la présente demande d'information " ne doit pas être considérée comme un engagement à émettre une demande subséquente ". Il est donc important de noter que la section 2.3 représente le calendrier prévu de la demande de proposition si le Canada passe à cette étape. Le processus de demande de propositions, et plus particulièrement le plan d'évaluation des offres, n'a pas encore été entièrement déterminé. Il dépendra en partie des commentaires reçus de l'industrie au cours du processus de demande d'information. Toute contribution sur la meilleure façon de procéder afin d'obtenir une solution offrant le meilleur rapport qualité-prix par le biais d'un processus

d'approvisionnement équitable et objectif est la bienvenue. Pour l'instant, nous n'avons pas l'intention de présélectionner les fournisseurs potentiels, mais nous envisageons inclure une partie de démonstration dans le processus d'évaluation des offres. Cette démonstration servirait à évaluer l'expérience utilisateur des solutions proposées par rapport à un ensemble prédéterminé de fonctions clés de gestion des risques définies dans les spécifications des exigences logicielles. On s'attend à ce que toutes les solutions nécessitent un certain niveau de configuration pour répondre pleinement aux exigences du Canada. Ces démonstrations dans le cadre de l'évaluation de l'offre se concentreront probablement sur les fonctions communes de gestion des risques de haut niveau que l'on attend d'une solution commerciale. Elles pourraient également servir à évaluer la maturité de la solution proposée afin de réduire au minimum le risque de développement et de s'aligner autant que possible sur les logiciels commerciaux existants.

Q11 : La demande d'offre contient des références au contenu qui est hébergé sur les sites intranet du MDN (c.-à-d. page 34 de l'annexe B). Si cette information fait également partie des exigences de la DDR, peut-elle être fournie directement ?

R11 : Oui, c'est possible. Si une certaine documentation est requise afin de fournir un meilleur retour d'information pendant la demande d'information, alors le Canada peut fournir les références. Toutes les références seront disponibles si le Canada procède à une demande de proposition.

Q11a : Devrions-nous dresser une liste des documents qui, selon nous, pourraient nous aider à élaborer notre réponse ?

R11a : Les répondants peuvent demander des références trouvées sur les sites intranet du MDN en soumettant leur demande au courriel de contact de la DDR, et l'autorité contractante peut fournir les documents demandés.

Q12 : Veuillez expliquer ce que l'on entend par "risque par défaut" par opposition aux domaines de risque spécifiques énumérés à l'appendice 4 de l'annexe B ?

R12 : Les risques par défaut établissent la base des informations minimales requises pour soulever un risque ou une opportunité sans soulever un risque en utilisant l'un des domaines de risque spécifiques. On ne s'attend pas à ce que ce type de risque soit largement utilisé, mais il donne la possibilité à un utilisateur de soulever un risque de base même s'il n'est pas sûr du domaine spécifique à utiliser. Idéalement, la solution logicielle de gestion des risques permettrait simplement au Canada de créer et de personnaliser différents types de risques et d'opportunités.

Q13 : Le MDN a-t-il une date cible pour la mise en œuvre / mise en service de la solution ?

R13 : Pour le moment, nous n'en avons pas. On s'attend à ce que cette date soit déterminée en collaboration dans le cadre de l'élaboration du calendrier du projet PM-001. Évidemment, comme cette solution est destinée à être déployée dans un environnement en nuage géré par le MDN (un abonnement à Microsoft Azure), un certain nombre d'étapes dépendent de la contribution du Canada. Nous avons énuméré les activités et les jalons clés dans la description des éléments de données du livrable PM-001 qui détermineront le calendrier général et le jalon de mise en service éventuel.

Q14 : Le suivi des problèmes et des incidents fera-t-il partie de cette exigence ?

R14 : Actuellement, le suivi des problèmes et des incidents ne fait pas partie de notre champ de fonctions obligatoires, mais c'est quelque chose que nous pouvons considérer comme un atout.

Q15 : Quel est le processus de rétroaction après la soumission de la DDR ?

R15 : Actuellement, le MDN n'a pas l'intention de s'engager davantage avec l'industrie. Nos intentions demeurent alignées sur le calendrier proposé à la section 2.3 de la DDR, mais des DDR de suivi (y compris des ébauches de DP) pourraient être émises.

Q16 : Quel est votre objectif à avoir tous les domaines de risques dans une seule base de données plutôt que dans plusieurs espaces dédiés ?

R16 : L'objectif est de pouvoir générer une liste des risques associés à un projet, un programme ou une plate-forme donnés (par exemple), quel que soit leur domaine. Par exemple, un projet peut comporter des risques liés à la sécurité, des risques liés au projet et des risques liés aux munitions et aux explosifs. Cela permettrait au projet de gérer ses risques consolidés et d'évaluer son niveau de risque global en fonction de tous les types de risques. Les données associées aux différents domaines de risques peuvent être stockées dans des bases de données séparées en arrière-plan.

Q17 : Est-il nécessaire de suivre la conformité de la séparation des tâches entre les rôles autorisés ?

R17 : Oui. Nous avons besoin de la séparation des tâches et des contrôles sur les rôles autorisés. En tant que tel, un suivi est nécessaire. Cela fait partie de quelques contrôles de sécurité clés qui doivent être mis en œuvre dans le cadre du processus d'évaluation et d'autorisation de la sécurité.

Q18 : Comment le MDN gère-t-il les risques de la DDR et d'autres risques commerciaux aujourd'hui ?

R18 : Les risques et les possibilités du projet et du programme : Les politiques sont définies et référencées dans les spécifications des exigences logicielles. Il n'y a pas de processus spécifiques ni d'outils mandatés. Les projets d'immobilisations rendront compte des risques de haut niveau aux conseils supérieurs par l'entremise du module du système de projet dans l'outil de planification des ressources de l'entreprise du MDN. Toutefois, la gestion et l'analyse quotidiennes des risques sont effectuées de façon ponctuelle par l'équipe de projet au moyen de feuilles de calcul Excel ou de SharePoint, ou sont confiées à l'industrie. Les opportunités sont rarement suivies.

Risque de sécurité et cybersécurité : Les politiques sont définies et référencées dans les spécifications des exigences logicielles. Il n'existe pas de processus spécifiques ni d'outils obligatoires. Comme pour les risques liés aux projets et aux programmes, ils font généralement l'objet d'un suivi ad hoc sur des feuilles de calcul Excel.

Risques liés à la sécurité des munitions et des explosifs : Une politique et un processus existent à cet égard, mais il n'y a pas d'outils obligatoires. En fin de compte, ces risques sont saisis dans des documents Word qui sont soumis pour examen et approbation.

Risques liés au matériel naval en service : Il existe des politiques, des processus et des outils obligatoires à cet égard, mais la méthode et les outils actuels ne sont pas les plus efficaces et ne permettent pas une gestion efficace des risques. Ces risques commencent par l'examen d'un dossier de gestion des risques (document Word), puis les informations de ce document sont copiées/collées dans une notification via le module de maintenance de SAP. Cette notification est ensuite soumise à l'examen (par le biais d'un changement de statut) des parties prenantes. L'approbation/approbation officielle se fait par l'envoi d'un message militaire par l'autorité opérationnelle. Ce message est ensuite copié/collé dans la notification dans SAP.

Risques liés à la navigabilité : Il existe des politiques, des processus et des outils obligatoires à cet effet. Le processus commence généralement par des notifications par courriel et est suivi par le suivi des risques à l'aide de l'outil actuel Microsoft Access soutenu par une base de données SQL. Tous les aspects ne sont pas réalisés par l'intermédiaire de l'outil Microsoft Access et, par conséquent, des documents Word sont encore utilisés lorsque cela est nécessaire. Le processus de gestion des risques liés à la navigabilité commence par l'identification des risques. Lorsque le risque est identifié, une évaluation de l'impact de la navigabilité est effectuée pour déterminer l'indice du niveau de risque. Si l'indice de niveau de risque est supérieur au niveau de sécurité acceptable (ALOS), une notification d'alerte de risque (RAN) est envoyée à toutes les parties prenantes (par courrier électronique). L'autorité compétente accuse ensuite réception du RAN. Dans les 24 heures suivant

l'émission du RAN, une alerte de risque de navigabilité (ARA) est rédigée et émise. L'objectif de l'ARA est d'informer toutes les parties prenantes de la situation (risque et niveau de confiance), des mesures prises pour déterminer le niveau de risque réel et de toute action d'atténuation prévue ou en place comme mesure provisoire. L'étape finale consiste à rédiger l'enregistrement de la gestion des risques liés à la navigabilité (RARM) pour saisir (dans les 14 jours suivant l'ARA), identifier et gérer les problèmes de risques liés à la navigabilité, y compris les activités d'atténuation. L'ARA et le RARM sont formellement documentés dans la base de données MS Access et la base de données est également utilisée pour suivre les activités d'atténuation. Les copies signées des évaluations des risques (ARA et RARM) sont sauvegardées dans un autre référentiel. Si le risque n'est pas approuvé, une nouvelle version du RARM doit être émise, ce qui constitue une exigence de navigabilité. En outre, un plan d'action doit être suivi pour la stratégie d'atténuation des risques afin de respecter les délais.

Q19 : Quel cadre de gestion des risques utilisez-vous aujourd'hui ?

R19 : Le cadre stratégique de gestion du risque est celui élaboré par le Conseil du Trésor : https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=19422. Ce cadre fournit des conseils aux administrateurs généraux sur la façon de mettre en œuvre des pratiques efficaces de gestion des risques à tous les niveaux de leur organisation.

Q20 : Comment gérez-vous les rapports sur les risques de l'entreprise aujourd'hui ?

R20 : Les rapports sur les risques de l'entreprise se font principalement par le biais de l'outil de planification des ressources de l'entreprise du MDN à un niveau supérieur. Cependant, l'objectif de ce logiciel de gestion des risques est de permettre une meilleure gestion des risques au niveau tactique, et donc d'accroître notre compréhension stratégique du niveau de risque. Il n'est pas destiné à établir des rapports sur les risques au niveau de l'entreprise (MDN), même si les données influenceront évidemment ces rapports.

Q20a : Les simulations feront-elles partie de l'exigence ?

R20a : Non, il n'y a pas d'exigences spécifiques pour les simulations.

Q21 : Quel est le volume des risques que vous envisagez de gérer ?

R21 : Comme il n'existe actuellement aucune solution unique pour gérer efficacement les risques, ce nombre est difficile à déterminer. Ce nombre variera aussi considérablement en fonction du niveau d'adoption par les divers organismes et projets. La base de données actuelle sur les risques liés à la navigabilité compte un total d'environ 2,600 risques. On estime qu'il y aura 200 risques actifs liés au matériel naval, 50 risques actifs liés à la sécurité et à la cybersécurité, 20 risques actifs liés à la sécurité des munitions et des explosifs, et 2 000 risques et opportunités actifs liés à la gestion des projets et des programmes.

Q22 : Quels sont les domaines d'activité à risque que vous prévoyez d'aborder, outre ceux mentionnés dans la RFI ?

R22 : Aucun en dehors de ce qui est mentionné dans la DDR. On s'attend à ce que, à mesure que le Canada perfectionne sa façon de gérer les risques, des capacités ou des changements futurs soient nécessaires. Dans le cadre de ce marché, il y aurait une disposition pour les tâches émergentes afin de combler ces lacunes.

Q23 : À quelle fréquence procédez-vous à des évaluations des risques ? Est-ce fait annuellement, ou au besoin ?

R23: Cela dépend du type de risque. En général, la plupart des projets ayant de bonnes pratiques de gestion des risques effectuent une évaluation des risques au moins une fois par mois (selon la complexité du projet). Les risques liés à la sécurité et à la cybersécurité sont effectués régulièrement (le calendrier dépend du profil de risque du système en matière de confidentialité, d'intégrité et de disponibilité) et au besoin lorsqu'une vulnérabilité est identifiée. Les risques liés au matériel naval sont soulevés et évalués au besoin (lorsqu'un nouveau risque est identifié). Les risques liés à la navigabilité sont évalués selon les besoins (une fois qu'un nouveau risque est identifié) pour chaque flotte. En moyenne, environ 20 à 30 nouvelles évaluations de risques sont générées et enregistrées dans l'outil actuel (base de données MS Access) chaque année. Tout au long de leur cycle de vie, les évaluations des risques sont régulièrement mises à jour/révisées afin de saisir les nouvelles informations nécessaires.

Q24 : Combien d'objets/actifs veulent-ils suivre ?

R24 : Les spécifications des exigences logicielles comprennent une liste de toutes les flottes d'aéronefs et de toutes les classes de navires pour lesquelles le Canada veut être en mesure d'évaluer les risques. De plus, les exigences comprennent également la nécessité de suivre les risques au niveau de l'équipement avec des listes prédéterminées. De plus, on s'attend à ce que le logiciel soit nécessaire pour suivre des centaines de projets et de programmes contre lesquels des risques seraient soulevés.

Q24A : Avez-vous une hiérarchie des aéronefs et des navires ? Par exemple, les risques sont-ils suivis jusqu'à la hiérarchie de l'équipement/matériel, ou sont-ils suivis au niveau de l'actif/du projet ?

A24A : Nous avons besoin d'avoir la capacité de suivre les risques au niveau de la flotte/classe, au niveau de la plate-forme/avion individuel et au niveau de l'équipement. Les listes pour chacun de ces niveaux sont incluses dans les spécifications des exigences logicielles.

Q25 : Nous pensons que vous travaillerez avec un intégrateur de systèmes, et que le fournisseur de logiciels fournira des conseils de conception et participera au projet. Recherchez-vous également des services gérés ?

R25 : Puisque ce logiciel n'est pas destiné à être intégré au-delà de l'intégration nécessaire dans l'environnement en nuage (pour l'authentification et le SMTP par exemple), nous n'avons pas l'intention d'avoir un intégrateur de système distinct. Les tâches identifiées dans la section 3.2 de l'énoncé des travaux visent à aider le MDN à exécuter la gamme complète des fonctions requises pour déployer et configurer le logiciel de gestion des risques dans l'environnement en nuage géré par le MDN (abonnement à Microsoft Azure).

Q26 : La solution de gestion des risques devrait s'intégrer à d'autres solutions logicielles (comme SAP). Quelles autres solutions logicielles pourraient éventuellement être intégrées à la solution de gestion des risques ?

R26 : L'intégration réelle avec des solutions externes est actuellement hors de portée. Oui, on s'attend à ce qu'un jour l'intégration soit faite avec le logiciel de planification des ressources d'entreprise du MDN, qui est basé sur SAP. Nous prévoyons également que le logiciel de gestion des risques s'intégrera à d'autres outils qui sont, ou seront, déployés dans le grand environnement de données intégrées basé sur les systèmes infonuagiques.

Q26A : Vous attendez-vous à ce que l'entrepreneur effectue tout le travail de configuration dans votre environnement, ou travaillera-t-il de concert avec le MDN pour effectuer ce travail ?

R26A : On s'attend à ce que l'entrepreneur effectue le déploiement et la configuration de la solution dans l'abonnement infonuagique géré par le MDN pendant la phase de mise en œuvre. Pour ce faire, le MDN fournira à l'entrepreneur un accès privilégié à l'abonnement. Le MDN participera à la surveillance et au soutien des travaux, au besoin.

Q27 : Quelle est la classification des données, tant des éléments de données individuels que des données dans leur ensemble ?

R27 : La section 3.7.3 des spécifications des exigences logicielles traite des exigences de sécurité. Les éléments individuels peuvent avoir une classification allant jusqu'à Protégé B. On ne s'attend pas à ce que l'agrégation des données mène à une classification supérieure à Protégé B.

Q28 : Quelle est la classification de sécurité des systèmes sources susceptibles d'être intégrés à la solution de gestion des risques ?

R28 : Les systèmes sources seront au maximum de niveau Protégé B (notre système de planification des ressources d'entreprise basé sur SAP).

Q29 : Dans le cadre de contrats de type soutien en service, le système est-il censé intégrer d'une manière ou d'une autre avec des solutions industrielles ?

R29 : Pour l'instant, ce n'est pas le cas. L'idée est de déployer cette solution dans notre environnement infonuagique géré par le MDN et de fournir un accès à l'industrie en fonction des besoins. La solution de gestion des risques, et ses données, seraient donc entièrement gérées par le MDN et lui appartiendraient. Cet approvisionnement est une étape vers un environnement de données intégré plus vaste, où le MDN gérera des solutions et des données intégrées et donnera accès à l'industrie pour qu'elle collabore à des programmes et à des projets en utilisant le même ensemble d'outils et de données. Cela comprend, mais sans s'y limiter, la collaboration par le biais des divers contrats de soutien en service.

Q30 : Combien d'utilisateurs auront accès au système ?

R30 : Conformément au paragraphe 3.2.1 des spécifications des exigences logicielles, nous demandons un minimum de 500 utilisateurs simultanés, et un minimum de 2000 utilisateurs ayant accès à l'application. Comme nous ne disposons pas actuellement d'une solution commune pour gérer correctement les risques dans tous les domaines mentionnés dans les exigences, ces chiffres sont difficiles à évaluer.

Q31 : Recherchez-vous un modèle de service géré dans lequel le fournisseur s'occupe de tous les aspects du déploiement de l'infrastructure en nuage, de la mise à niveau, de la gestion et de la configuration de l'application, ou recherchez-vous une permutation en nuage sur place, du point de vue du déploiement?

R31 : La vision est que cet achat vise à obtenir un logiciel qui sera déployé sur place (dans le cadre de l'abonnement infonuagique géré par le MDN). L'entrepreneur aurait accès à cet abonnement infonuagique afin de déployer et de configurer la solution. Une fois que la solution sera opérationnelle, elle sera remise au MDN qui en assurera la gestion tout au long de son cycle de vie. On s'attend à ce que le MDN paie des frais de maintenance annuels pour avoir accès aux futures versions du logiciel et pour que l'entrepreneur puisse régler les problèmes techniques, comme le prévoient les clauses standard du CCUA.

Q31a : Une fois le système en service, le MDN sera-t-il responsable de l'entretien et de la gestion du logiciel, ou cela sera-t-il confié à un entrepreneur dans le cadre du modèle de service ?

R31a : Pour l'instant, l'objectif est que le MDN soit responsable de la gestion du logiciel une fois qu'il sera opérationnel. Le MDN devra avoir accès aux futures versions et mises à jour du logiciel, mais il sera responsable de la gestion de la configuration de la solution dans l'environnement infonuagique géré par le MDN et du déploiement de ces futures versions et mises à jour. S'il y a un besoin de fonctionnalité supplémentaire, cela peut être fait par le biais de tâches émergentes dans le contrat.

Q31b : Avez-vous envisagé un modèle de services gérés ?

R31b : Oui, cela a été envisagé. L'objectif est de minimiser les coûts pour le MDN et les contribuables, et de migrer tous les services vers un seul bureau de service, où le MDN gérerait tous les logiciels déployés dans l'environnement infonuagique. Ce bureau de service et cette organisation de soutien informatique sont déjà en cours de création dans le cadre d'autres projets.

Q31c : L'approvisionnement envisagerait-il un logiciel en tant que service (SaaS) au lieu d'une solution sur site ?

R31c : Actuellement, le MDN envisagerait un SaaS, mais les exigences actuelles prévoient l'acquisition d'une solution sur place pour plusieurs raisons. Une solution sur site :
a. assure un contrôle complet et unique des données (en transit et au repos), d'autant plus qu'elle contiendra des biens contrôlés et des données jusqu'au niveau Protégé B ;

b. permet une intégration facile avec l'Active Directory géré de manière centralisée et utilisé par d'autres applications similaires ;

c. permet une intégration facile avec d'autres applications colocalisées dans le même abonnement, tant du point de vue de l'API que de l'accès à la base de données, et ce sans avoir à exposer des données en dehors de l'abonnement géré par le MDN ;

d. permet de gérer le contrôle d'accès basé sur les rôles de manière centralisée en utilisant des rôles qui peuvent attribuer un accès prédéterminé aux utilisateurs pour un certain nombre d'applications ;

e. réduit les risques de sécurité informatique liés au transfert constant de données en dehors de l'abonnement (par Internet)

f. réduit la duplication des coûts associés à la surveillance de la sécurité et à d'autres fonctions administratives qui doivent déjà être assurées par le MDN pour d'autres applications déployées dans le même abonnement.

Par conséquent, il ne s'agit pas de dire qu'une solution SaaS ne pourrait pas répondre aux aspects ci-dessus, mais cette approche comporte un certain nombre de risques inhérents. S'il s'agissait d'un achat unique sans intention d'intégrer la solution à d'autres applications, nous opterions probablement pour une approche SaaS plutôt que sur site.

Q32 : Les exigences portent spécifiquement sur Microsoft Azure, y a-t-il une raison pour laquelle d'autres fournisseurs infonuagiques publics ne seraient pas considérés ?

R32 : Bien que le gouvernement du Canada puisse mettre en place des contrats avec tous les principaux fournisseurs infonuagiques publics (Google, Amazon Web Services, Microsoft Azure), un abonnement à Microsoft Azure est déjà en place là où d'autres projets sont actuellement déployés et sont des cibles pour l'intégration avec le logiciel de gestion des risques. Afin de réduire la complexité et les risques de sécurité informatique liés au transfert de données entre les abonnements, l'objectif est de déployer le logiciel de gestion des risques au sein de l'abonnement Azure existant.

Q33 : Quel est le budget de ce contrat ?

R33 : Le budget dépendra de la rétroaction de l'industrie par le biais de l'une des questions clés de l'annexe E. Cette question de l'annexe E est importante pour le MDN afin de trouver le financement approprié avant de lancer la demande de proposition. Ce contrat n'est pas destiné à être un projet capital (d'une valeur supérieure à 4,5 millions de dollars). Compte tenu des exigences actuelles, de l'objectif de tirer parti autant que possible des logiciels commerciaux et du fait que l'intégration à d'autres solutions est hors de portée, le Canada s'attend à ce que le budget requis pour ce marché soit bien inférieur au seuil de 4,5 millions de dollars. Le budget global doit également prendre en compte la mise en œuvre, les licences et le maintien de la solution, car tout cela fait partie de la valeur globale du contrat. Ces aspects seront tous calculés, comme on peut le voir dans le projet de proposition financière (annexe C) qui a été fourni avec la demande d'information.

Q33a : Le type de financement (capital ou maintenance) sera-t-il affecté par le modèle d'abonnement ?

R33a : Oui, on s'attend à ce qu'il y ait un certain impact. Les travaux de mise en œuvre initiale ainsi que les licences à vie sont financés par des fonds capitaux. Les licences d'entretien et les licences récurrentes sont acquises à l'aide de fonds de maintenance. Bien que la préférence du Canada soit d'obtenir des licences à vie pour un nombre

illimité d'utilisateurs (ce qui facilite l'adoption à grande échelle et offre probablement un bon rapport qualité-prix à long terme), les deux modèles sont actuellement offerts dans l'ébauche de la proposition financière (annexe C).

Q34 : Pourquoi la capacité de gestion des risques n'est-elle pas acquise dans le cadre du projet Défense X (modernisation du SIGRD) ?

R34 : La portée du projet Défense X (modernisation du SIGRD) est encore en cours de détermination. Par conséquent, nous ne savons pas si une capacité de gestion des risques répondant à nos besoins sera fournie dans le cadre de ce projet. L'intention de cet achat de logiciel de gestion des risques sera d'avoir une période initiale de contrat qui couvre l'écart jusqu'à ce que le projet Défense X soit mise en œuvre, puis des années d'option pour étendre la capacité afin de tenir compte d'une période de transition et des retards potentiels.

Q35 : Les dispositions de la clause CCUA 4002 (services de développement ou de modification de logiciels) ne sont pas alignées sur la nature d'une application SaaS. Quelle est la base des exigences liées au codage dans la clause 4002 des CCUA et peut l'effet souhaité être atteint grâce à un logiciel qui a été conçu de manière efficace pour permettre la configuration du client?

R35 : Selon R31c, la vision est que cet approvisionnement vise ultimement à obtenir un logiciel qui sera déployé sur place (dans le cadre de l'abonnement infonuagique géré par le MDN). Le contractant aurait accès à cet abonnement cloud afin de déployer et de configurer la solution. Une fois opérationnel, il serait remis au MDN pour être géré tout au long de son cycle de vie. On s'attend à ce que des frais de maintenance annuels soient payés par le MDN afin d'avoir accès aux futures versions du logiciel et pour que l'entrepreneur règle les problèmes techniques, comme stipulé dans les clauses standard des CCUA.

Malgré l'approche de déploiement sur site, le MDN a l'intention de minimiser autant que possible toute personnalisation de l'application (changements de code) à moins que cela ne soit absolument nécessaire. L'idée serait de se procurer une solution qui permette la flexibilité grâce à la configuration disponible dans l'application. Cette approche garantira que le MDN est en mesure de passer facilement aux futures versions de l'application dès qu'elles seront disponibles.

Q36 : Avez-vous envisagé d'énoncer des exigences concernant les données et la base de données de sorte que le Canada puisse facilement extraire les données et les importer dans une nouvelle solution logicielle si vous décidez de changer de fournisseur de logiciel en cours de route ?

R36 : Oui. Le paragraphe 3.7.5.1.1 des spécifications des exigences logicielles stipule que "les données générées par le logiciel de gestion des risques ne doivent pas dépendre de l'utilisation d'une application propriétaire commerciale spécifique". Il s'agit de permettre au

Canada un accès complet et complet à ses données à tout moment, quelle que soit l'application utilisée pour effectuer la gestion des risques.

Q37 : Comment pourrions-nous (en tant que fournisseur de logiciels) être responsables des problèmes de logiciels si le Canada a la capacité de modifier le code du logiciel ?

R37 : Le Canada n'a pas l'intention de modifier le code du logiciel. C'est notre intention d'indiquer clairement que les clauses contractuelles concernant la modification du code s'appliquent aux scripts de déploiement personnalisés qui doivent être développés dans le cadre de ce contrat où la propriété intellectuelle appartiendrait au Canada.

Q38 : Comment ferions-nous (en tant que fournisseur de logiciels) pour nous assurer que notre propriété intellectuelle est protégée si nous permettions au Canada de modifier le code, ce qui nécessiterait un accès complet à la propriété intellectuelle associée au logiciel.

R38 : Le Canada a l'intention de respecter la propriété intellectuelle qui appartient à un fournisseur de logiciels, en particulier en ce qui concerne le logiciel de gestion des risques de base. Cependant, la propriété intellectuelle de tout script ou code personnalisé qui serait développé dans le cadre de ce contrat appartiendrait au Canada.

Q39 : Comment comptez-vous appliquer les clauses de gestion de la qualité qui permettent d'encadrer l'évolution du code ?

R39 : Le Canada n'a pas l'intention de superviser le développement et le codage du fournisseur qui se rapporte au logiciel de gestion des risques. La clause CCUA 4002 vise à fournir la capacité de superviser le développement de scripts ou de codes personnalisés qui seraient développés dans le cadre de ce contrat, et de superviser le déploiement et les tests du logiciel dans l'environnement infonuagique géré par le MDN.

Q40 : Nous notons que le Canada exige que le fournisseur du logiciel s'acquitte de la fonction de gestion de projet pour la mise en œuvre de la solution logicielle et prévoit que le Canada cherchera à gérer le projet des changements de processus associés au sein du GPEM et du GPEA. Quelle serait la capacité du fournisseur de charger et de gérer les ressources humaines du MDN dans les divers départements des parties prenantes nécessaires à la réalisation du projet?

R40 : Le Canada n'a pas l'intention de confier toutes les fonctions de gestion de projet à l'entrepreneur. Le Canada demeurera le principal gestionnaire de projet pour ce projet. Cependant, en raison de pénuries de personnel, le Canada demande à l'entrepreneur d'exécuter plusieurs fonctions clés qui aideront le MDN à gérer le projet et à réduire les risques d'exécution. Ces fonctions et les produits livrables associés sont énumérés dans l'énoncé des travaux.

L'entrepreneur n'aurait pas le pouvoir d'assigner des ressources humaines à l'ensemble des services des divers intervenants. Le MDN fournira l'accès aux ressources clés pour soutenir l'entrepreneur et le calendrier établi autant que possible, dans les contraintes et les priorités de chaque département.

Q40a : L'entrepreneur aurait-il accès au système informatique du Canada?

R40a : L'entrepreneur aura un accès privilégié à l'abonnement infonuagique géré par le MDN afin d'effectuer les tâches de l'énoncé des travaux (notamment pour déployer et configurer la solution de gestion des risques).

Q40b : Comment le Canada abordera-t-il les conflits d'intérêts potentiels (par exemple, concernant la réalisation des avantages)?

R40b : Comme le Canada demeurera le gestionnaire de projet global pour l'exécution de ce projet, nous ne voyons aucun conflit d'intérêts potentiel.

Q41 : Est-ce que le Canada est intéressé à comprendre la portée plus large des capacités des fournisseurs potentiels et souhaiterait-il appliquer une pondération à cette portée?

R41 : Dans le cadre de cette demande d'information, le Canada accueille toute suggestion de fonctionnalités supplémentaires que nous devrions envisager d'inclure dans nos spécifications d'exigences logicielles afin de mieux gérer les risques. Ceux-ci peuvent être fournis via la réponse à la demande d'informations. Cependant, le Canada ne peut pas attribuer un poids aux capacités qui pourraient répondre à des exigences potentielles qui ne font pas partie de la portée de l'approvisionnement (au-delà des exigences obligatoires et souhaitables existantes).

C'est l'intention du Canada que le contrat qui en résulterait permettrait le mettre en place des tâches émergentes de sorte que toute nouvelle exigence (telle que de nouvelles capacités) puisse être satisfaite en cours de route. On s'attend à ce qu'il y ait plusieurs fonctionnalités présentement inconnues dont le Canada pourrait avoir besoin à l'avenir alors que nous continuons à faire évoluer certaines des politiques et des processus opérationnels liés à la gestion des risques. Lorsque ces fonctionnalités sont connues, des tâches émergentes peuvent être soulevées pour que l'entrepreneur développe une solution qui réponde au besoin.

Q42 : Le MDN recherche-t-il une solution COTS ?

R42 : Oui, le MDN recherche une solution COTS afin de minimiser les risques, de minimiser les coûts de mise en œuvre et de cycle de vie, et de réduire autant que possible le délai de mise en œuvre.

Q43 : Le MDN a-t-il tenu compte de toutes les normes gouvernementales pertinentes ?

R43 : Oui, le MDN a tenu compte des principales normes gouvernementales, telles qu'elles sont incluses dans nos spécifications des exigences logicielles. Outre les normes liées à la sécurité des TI, ces normes comprennent celles liées à l'accessibilité, à la convivialité et aux langues officielles.

Q44 : Le MDN peut-il expliquer plus en détail le concept de concentrateur ("hub") et rayon ("spoke") ?

R44 : Des détails sur le concept de zone d'atterrissage (ou locataire, ou hub) sont accessibles sur le site Web de Microsoft : https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/.

Dans le contexte du programme infonuagique de la défense, une zone d'atterrissage commune à l'entreprise du MDN (appelée le locataire ou le concentrateur) est disponible de façon centralisée pour tous les abonnements gérés par le MDN (ou rayons). Cette approche permet de fournir plusieurs services communs à partir du concentrateur vers les différents rayons (services tels que Active Directory et SMTP) ainsi que de fournir la sécurité de base pour gérer l'échange de données vers l'extérieur (à la fois vers Internet et vers le réseau sur site de la défense). En déployant le logiciel de gestion des risques dans l'un des rayons, nous héritons également d'un grand nombre de contrôles de sécurité mis en œuvre par le concentrateur, ce qui laisse environ 58 contrôles à mettre en œuvre par les rayons et les applications déployées dans les rayons. Cette approche permet donc de réduire les coûts et les risques liés à la sécurité informatique.

Q45 : Comment le MDN prévoit-il d'atteindre un Authorisation d'exploitation (AE) d'un mois ?

R45 : Cela peut être réalisé grâce au fait que le logiciel de gestion des risques serait déployé dans un environnement à rayons au sein d'un locataire (ou d'un concentrateur) infonuagique où un grand nombre de contrôles de sécurité seraient déjà hérités par le rayon. En outre, un certain nombre de projets parallèles sont en cours pour faire mûrir cet environnement afin qu'il puisse atteindre un AE pour Protégé B. Cela contribuerait à raccourcir l'AE associé au logiciel de gestion des risques.

Q46 : La DP acceptera-t-elle les offres des fournisseurs de logiciels seulement ou celles des revendeurs également ?

R46 : Si le Canada passe à l'étape de la DP, l'intention serait d'accepter les offres des fournisseurs de logiciels en tant que soumissionnaires ou des revendeurs en tant que soumissionnaires. L'offre recommandée pour l'attribution du contrat pourrait éventuellement être un

partenariat où un fournisseur effectuera le travail et livrera un logiciel tiers dont il a obtenu les droits de vente au Canada de la part de l'entreprise du vendeur de logiciels.

Q47 : Quel est le calendrier de la demande de propositions ?

R47 : Conformément à la demande de renseignements, si une demande de propositions subséquente est émise, l'objectif actuel est de lancer la demande de propositions entre la mi-septembre et la fin septembre, de sorte que l'évaluation des offres puisse être effectuée en novembre et qu'un contrat soit attribué en décembre. Évidemment, plusieurs facteurs pourraient prolonger ce délai, mais c'est l'objectif actuel de l'équipe.

Q48 : La gestion des risques financiers (c'est-à-dire la vérification/le filtrage des achats) est-elle incluse dans le champ d'application de cette DDR ?

R48 : Les risques du projet et du programme peuvent être directement liés au budget/aux finances. Ceux-ci peuvent inclure des risques associés aux efforts d'approvisionnement pour soutenir le projet ou le programme associé.

Q49 : Comment le risque du fournisseur et l'évaluation des risques associés aux tiers sont-ils pris en compte dans cette demande ? (par exemple, risque réglementaire et de réputation, filtrage des sanctions, surveillance des nouvelles négatives, exposition étrangère défavorable, etc.)

R49 : Selon R48, les risques associés aux efforts d'approvisionnement pour un projet ou un programme relèveraient des risques du projet et du programme.

Q50 : Est-il nécessaire de comprendre les bénéficiaires effectifs, les principales personnes de contrôle et les structures de propriété des fournisseurs/entrepreneurs ?

R50 : Non, il n'est pas nécessaire de fournir plus que ce qui serait requis pour appuyer le processus d'habilitation de sécurité du gouvernement du Canada.

Q51 : Les données et analyses sur les risques climatiques sont-elles incluses dans le champ d'application de cette DDR ?

R51: Non, ils ne le sont pas.

Q52: Si un ensemble combiné de risques identifiés dans cette DDR va au-delà des solutions spécifiques de notre entreprise, le gouvernement envisagera-t-il une réponse combinée avec nos partenaires de confiance offrant une approche modulaire ?

R52 : Selon A46.
Le Canada préférerait avoir un accord de licence du revendeur, même si plus d'un fournisseur tiers peut être impliqué dans la fourniture de la solution.

Q53 : Le gouvernement peut-il fournir une liste d'exemples de risques/problèmes qu'il cherche à prévenir avec un appel d'offres potentiel ?

R53 : L'objectif de ce marché est d'obtenir un logiciel de gestion des risques permettant au MDN de relever, de suivre et de gérer les risques à un niveau tactique. Cela éclairera à son tour la prise de décision au niveau stratégique et de l'entreprise. Ce logiciel sera utilisé pour aider le MDN à mieux gérer les divers types de risques à l'appui des processus opérationnels sous l'égide de l'acquisition et du soutien du matériel.

Q54 : Nous considérons que bon nombre de nos fonctionnalités sont uniques. Le gouvernement tiendra-t-il compte de l'une ou l'autre des exigences particulières en vertu de l'autorisation à fournisseur unique?

R54 : Non, le Canada ne tiendra pas compte des exigences relatives à un fournisseur unique dans le cadre de cette exigence. Toute exigence supplémentaire qui, selon les répondants, devrait être ajoutée dans le cadre de la spécification des exigences logicielles ou de l'énoncé des travaux doit être soumise au Canada via la réponse à la DDR afin qu'elle puisse être prise en considération.

TOUS LES AUTRES TERMES ET CONDITIONS RESTENT INCHANGÉES.