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

SCHL CMHC

schl.ca

Questions des proposants et réponses de la SCHL

DDP 002376 – Solution en matière de gouvernance, de gestion des risques et de conformité (GRC)

Date : 14 mars 2024

QUESTIONS ET RÉPONSES – 3

TABLEAU DES QUESTIONS ET DES RÉPONSES

N°	Question du proposant	Réponse de la SCHL
1	Pouvons-nous soumettre deux propositions distinctes afin de fournir à la SCHL deux solutions de GRC distinctes?	Chaque système devra faire l'objet d'une soumission distincte et sera évalué séparément.
2	Veuillez énumérer et décrire brièvement l'infrastructure technique, la technologie et les outils actuellement utilisés dans les différentes étapes du cycle de vie des données. De la création ou de l'intégration de données à la destruction ou à l'archivage des données par des personnes qui occupent certaines fonctions, y compris l'analytique, les responsables des données, les utilisateurs de Power BI, etc.	La SCHL ne fournira pas cette information pour le moment.
3	Veuillez énumérer et décrire les scénarios, les méthodologies, les méthodes et les outils de haute disponibilité des données et de reprise après sinistre actuellement en place, y compris la géodistribution et l'architecture multientité.	La SCHL ne fournira pas cette information pour le moment.
4	Pourriez-vous décrire les données dans les systèmes actuels en fonction des éléments suivants :	Le seul système remplacé par la solution de GRC proposée est le système d'audit (TeamMate+).

	• Volume – la quantité de données (To, enregistrements, entités, transactions, utilisateurs et clients uniques et toute autre mesure correspondante); • Variété – le nombre de types et de genres différents de données (domaines de données, entités, attributs); • Vitesse – la vitesse de génération, de modification et de traitement des données (Go, enregistrements, transactions par année, mois, jour, heure, seconde).	La SCHL a environ 225 fichiers de projets d'audit antérieurs dans TeamMate+ et n'a pas d'autres données importantes (données sur les risques, données de contrôle) qui doivent être migrées pour l'audit. La taille du fichier de la base de données est d'environ 40 Go. La SCHL ne migre qu'un ensemble de données actives (environ 10 ans de données).
5	Y a-t-il des politiques de conservation des données en place?	Pour les dossiers d'audit et de risques, voir 4.4.1 g) – période de conservation de 10 ans après la dernière modification du dossier.
6	Veuillez énumérer et décrire brièvement les postes opérationnels et techniques qui interviennent aux différentes étapes du cycle de vie des données pour les systèmes actuels.	La SCHL ne fournira pas cette information pour le moment.
7	Veuillez énumérer et décrire, si nécessaire, les moyens actuels d'accès aux données : les applications de bureau intégrées, les portails Web, les applications mobiles, les agents conversationnels, l'analytique intégrée, les courriels, le matériel particulier, etc.	La SCHL ne fournira pas cette information pour le moment.
8	Y a-t-il des limites liées à la migration, comme la disponibilité et la durée des éventuels temps d'arrêt?	La migration des données d'audit devrait avoir lieu dans le cadre de la mise en œuvre du nouveau système et consistera principalement en une migration des données historiques. On s'attend donc à ce qu'il n'y ait pas de restrictions importantes liées à la disponibilité/aux temps d'arrêt pendant la migration.

9	Selon ce que nous avons déjà répondu à des demandes de soumissions semblables du gouvernement du Canada pour des solutions de logiciel-service, il existe généralement des exigences fonctionnelles et non fonctionnelles obligatoires pour garantir la conformité des soumissionnaires. De plus, la méthode d'approvisionnement de logiciels-services (DAMA) du gouvernement du Canada fournit un ensemble d'exigences de sécurité obligatoires approuvées par le Centre canadien pour la cybersécurité (CCC) afin d'évaluer une offre de logiciel-service Protégé B (lien vers l'affichage : DAMA - Méthode d'approvisionnement de logiciels-services (Infonuagiques GC) – Avis d'appel d'offres | AchatsCanada). La Couronne envisagerait-elle d'ajouter les exigences obligatoires approuvées par le CCC pour les logiciels-services de type Protégé B, comme l'indique la méthode d'approvisionnement de logiciels-services du gouvernement du Canada (numéro de demande de soumissions EN578-191593/F)?	L'équipe de la Sécurité de la SCHL est favorable à ce que les proposants fournissent des preuves de solutions de sécurité supplémentaires dans leur réponse à la DDP. La SCHL ne modifiera pas les exigences obligatoires.
10	En ce qui concerne les solutions de logiciels-services de type Protégé B, le Centre canadien pour la cybersécurité (CCC) exige que les fournisseurs de logiciel-service se conforment aux certifications et rapports d'audit suivants, reconnus par l'industrie. ○ ISO/IEC 27001:2013 Technologies de l'information -- Techniques de sécurité -- Systèmes de gestion de la sécurité de l'information – Exigences; ○ ISO/IEC 27017:2015 Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage;	L'équipe de la Sécurité de la SCHL est favorable à ce que les proposants fournissent des preuves de solutions de sécurité supplémentaires dans leur réponse à la DDP. La SCHL ne modifiera pas les exigences obligatoires.

	○ ISO/IEC 27018:2014 Technologies de l'information, Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII; Certification Service Organization Control (SOC) 2 Type II pour les principes de confiance que sont la sécurité, la disponibilité, l'intégrité du traitement et la confidentialité. ○ La Couronne envisagerait-elle d'ajouter une exigence obligatoire selon laquelle les fournisseurs doivent fournir ces attestations avec la soumission afin de démontrer la conformité à l'exigence visant les logiciels-services de type Protégé B?	
11	En ce qui concerne l'exigence cotée C1.7 dans la section Expérience et compétences de l'organisation de la DDP, la Couronne peut-elle confirmer ce qui suit : a. Si les soumissionnaires sont tenus de fournir des rapports SOC 2 de type II? b. Si les soumissionnaires peuvent fournir la page de résumé du rapport au lieu du rapport complet? (en raison des informations sensibles, le rapport n'est généralement pas partagé).	Un rapport complet SOC 2 de type II n'est pas requis. Les proposants peuvent fournir une page de résumé qui prouve ou valide qu'ils répondent aux exigences de certification/d'attestation.
12	En ce qui concerne l'exigence cotée C1.4 sous Expérience et compétences de l'organisation, la Couronne peut-elle fournir une définition de ce qui est considéré comme une grande organisation	Pour l'instant, la SCHL ne donne pas de définition normative à l'expression « grande organisation complexe ». Les proposants sont encouragés à faire leurs propres choix conformément à l'exigence cotée C.1.4 :

	complexe? (C.-à-d. en fonction du nombre d'employés, des revenus annuels, etc.)	« Éventail de clients dans le domaine des solutions de logiciel-service de gouvernance, de gestion des risques et de conformité. Mentionnez au moins deux (2) organismes publics et de grandes organisations complexes comme des institutions financières ou des assureurs hypothécaires. »
13	La section 2.2.1, Notation par le comité d'évaluation, de la DDP comprend un tableau qui présente la façon dont les critères cotés sont notés. La Couronne peut-elle confirmer que chaque critère évalué dans les sections C.1 Expérience et compétences de l'organisation, C.2 Approche et méthodologie et C.3 Expérience et compétences des ressources proposées valent un maximum de 5 points chacun, comme l'indique le tableau de notation de la section 2.2.1?	Les critères cotés (C.1 à C.4) et la présentation seront évalués à l'aide de la grille de notation fournie à la section 2.2.1. La pondération des critères cotés est énoncée à la section J de la DDP (mise à jour au moyen de la modification n° 2). Par souci de clarté, C.1 a une pondération de 5 %, C.2 a une pondération de 10 % et C.3 a une pondération de 5 %.
14	Afin de garantir l'équité et la transparence pour tous les fournisseurs, la Couronne peut-elle confirmer que chaque sous-exigence des sections cotées C.1 à C.3 est pondérée de manière égale? Par exemple, C.1 Expérience et compétences de l'organisation comporte 11 sous-exigences qui valent vraisemblablement 5 points chacune, de sorte que chaque exigence vaut 1/11 du total de 5 % de cette section.	Pour les critères cotés (C.1, C.2 et C.3), les sous-catégories seront évaluées selon la matrice de notation (0 à 5) fournie à la section 2.2.1 de la DDP. La moyenne des pointages des sous-catégories sera établie afin de fournir la note globale pour les critères cotés (C.1, C.2 et C.3).
15	Dans Devis estimatif, Tableau 1, élément 3 – Frais annuels, la Couronne peut-elle confirmer ses coûts annuels (pour être conforme à l'élément 4) et si la quantité doit être 3 pour la période initiale de trois ans?	Pour le coût annuel, la quantité doit être trois (3) et le COÛT UNITAIRE doit être le droit annuel. Le TOTAL EN $ CA AVANT TAXES correspond au total partiel (c.-à-d. QUANTITÉ X COÛT UNITAIRE = TOTAL EN $ CA AVANT TAXES).

16	Dans Devis estimatif, Tableau 1, élément 4 – Coûts du soutien continu, étant donné que la Couronne exige un coût annuel et que le tableau est pour une période de trois ans, la Couronne pourrait-elle envisager de mettre à jour le tableau Devis estimatif et d'obliger à mettre obligatoirement 3 comme quantité?	En ce qui concerne les coûts du soutien continu, s'ils ne sont pas inclus dans l'élément 3 – Frais annuels, la quantité (QTÉ) devrait être de trois (3) et le COÛT UNITAIRE serait le droit annuel des coûts du soutien continu. Le TOTAL EN $ CA AVANT TAXES correspond au total partiel (c.-à-d. QUANTITÉ X COÛT UNITAIRE = TOTAL EN $ CA AVANT TAXES).
17	Dans Devis estimatif, Tableau 1, élément 5 – Coûts de formation, la formation doit-elle être considérée comme un coût ponctuel pour la période de mise en œuvre?	Oui, il s'agit d'un coût ponctuel.
18	La Couronne peut-elle confirmer si la valeur totale du tableau 1 du Devis estimatif doit être la valeur totale de tous les coûts pour la période initiale de trois ans?	Oui, le sous-total du tableau 1 du Devis estimatif doit comprendre tous les coûts que le proposant a l'intention de facturer pendant la durée initiale de trois (3) ans de l'entente.
19	En nous fondant sur la plus récente modification visant l'évaluation et le classement des proposants, nous aimerions valider notre compréhension ci-dessous : a) Les notes obtenues pour (i) l'étape II CRITÈRES COTÉS et (ii) l'étape III DEVIS ESTIMATIF seront évaluées, et les quatre proposants les mieux classés passeront à l'étape suivante, soit l'étape IV PRÉSENTATION; b) Après la présentation, les quatre proposants les mieux classés seront évalués et notés en fonction des critères de présentation énoncés à la section K modifiée – Présentation;	Oui. Cette interprétation est exacte.

	c) Le fournisseur qui obtient la note la plus élevée à l'étape de la présentation reçoit une invitation écrite à entamer des négociations contractuelles directes. La Couronne peut-elle confirmer notre compréhension du processus et du classement des proposants?	
20	En ce qui concerne l'exigence 4.4.3, la Couronne peut-elle fournir un exemple de projet d'audit?	Les projets d'audit sont menés par la fonction indépendante d'Audit interne de la SCHL, dans le but de fournir au Conseil d'administration et à la haute direction de la SCHL une assurance, des observations et des conseils indépendants, objectifs et fondés sur les risques. Les projets d'audit sont généralement axés sur la gouvernance, la gestion des risques et le contrôle interne dans toute la fonction d'audit interne de la SCHL (p. ex., activités, processus, programmes, secteurs de risque, etc.).
21	Concernant la section 4.3.3 Évaluations, la Couronne peut-elle donner un exemple de hiérarchie des risques?	Une hiérarchie ou une taxonomie des risques est un ensemble complet, commun et stable de catégories de risques qui est utilisé au sein d'une organisation. En fournissant un ensemble *complet* de catégories de risques, elle encourage les personnes qui participent à l'identification des risques à tenir compte de tous les types de risques qui pourraient avoir une incidence sur les objectifs de l'organisation. La taxonomie de référence ORX et les catégories d'évènements de Bâle II en sont des exemples.
22	Concernant la section 4.6.5, la Couronne peut-elle fournir plus d'informations sur le système de renseignements personnels?	Infosource est le fichier de renseignements personnels de la SCHL. C'est une liste PDF publiée sur le site Web

		externe de la SCHL – INFO SOURCE 2023 – Sources de renseignements du gouvernement fédéral et sur les fonctionnaires fédéraux (cmhc-schl.gc.ca) Le système de GRC doit être en mesure de faire le suivi des renseignements suivants pour chaque programme ou produit : – si des renseignements personnels sont en jeu; – le numéro du fichier de renseignements personnels; - le code de rétention; - le lien vers l'évaluation des facteurs relatifs à la vie privée. Exemples sur le site Web de la SCHL : • Info Source 2023 PDF (FRANÇAIS) • Info Source 2023PDF
23	Requête concernant le numéro d'entreprise-approvisionnement (NEA). Je me suis inscrit sur le site https://mu.ariba.com/profile/org-profile pour obtenir le numéro. Est-ce exact ou faut-il faire autre chose pour obtenir le NEA?	L'inscription à SAP Ariba est comparable à l'inscription au NPF pour faire affaire avec le gouvernement du Canada. L'inscription à Services publics et Approvisionnement Canada (SPAC) est facultative, tout comme l'inclusion d'un numéro d'entreprise-approvisionnement (NEA) avec la proposition du proposant.