ANNEXE A - ÉNONCÉ DES BESOINS

1. Exigence gouvernementale

Emploi et Développement social Canada (EDSC), un ministère du gouvernement du Canada (Canada), a besoin d'un Système d'application de gestion des urgences (SAGU). Le SAGU doit être fourni comme logiciel en tant que service (SaaS) sur un nuage public capable de traiter des données de niveau Protégé B, ce qui facilitera la création, la surveillance, la gestion et la consolidation de l'information sur la gestion des urgences (p. ex., les plans) et des données (p. ex., coordonnées) dans les quatre piliers de la gestion des urgences (figure 1).

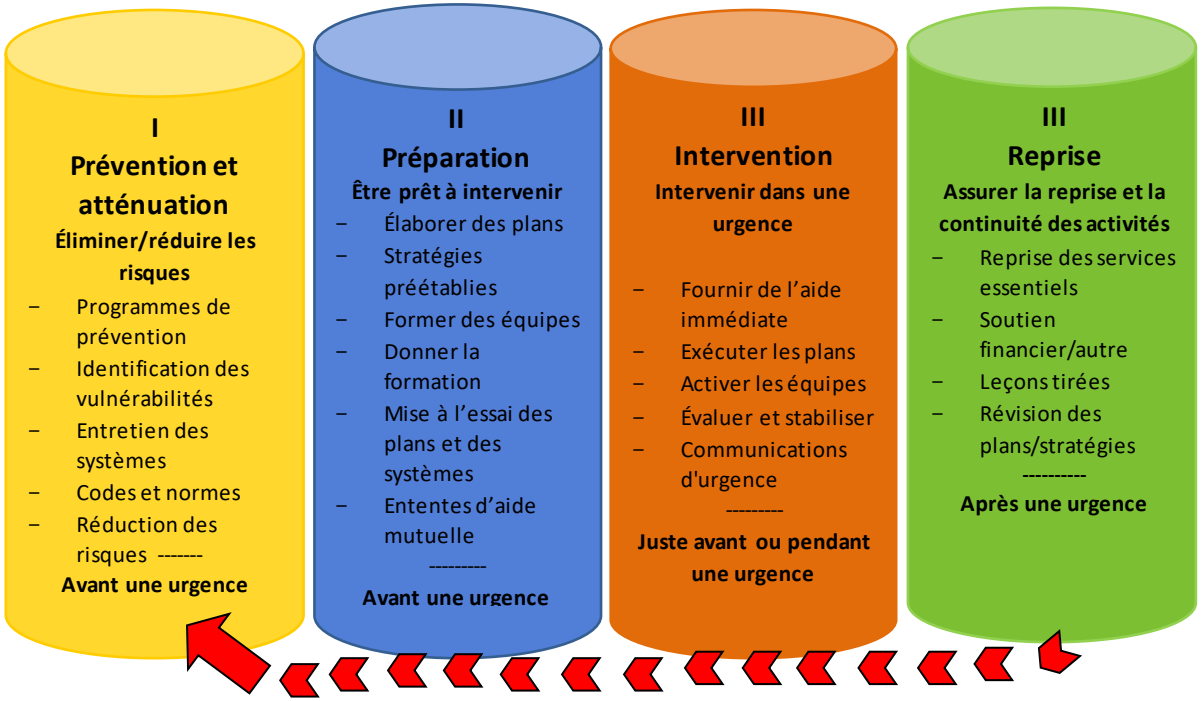


Figure 1 : Cycle de gestion des urgences (I. Prévention, II. Préparation, III. Intervention, IV. Reprise)

Le SAGU exige que les secteurs fonctionnels suivants, d'importance égale, appuient les quatre piliers de la gestion des urgences :

- Gestion de la continuité des activités
- Gestion de la continuité des activités de la TI
- Gestion de l'évacuation d'urgence de l'immeuble
- Gestion des crises et des urgences

Sans SAGU, les éléments susmentionnés représentent un défi logistique pour une organisation ayant la taille et la complexité d'EDSC. À titre de ministère fédéral, EDSC compte environ 30 000 employés, souvent gérés virtuellement, dans environ 490 emplacements au Canada, qui travaillent dans plusieurs secteurs d'activité. La Direction générale de l'innovation, de l'information et de la technologie (DGITT) d'EDSC fournit des services d'information et de technologie à EDSC, incluant les applications opérationnelles qui supportent et simplifient les méthodes de travail, l'accès aux données et le traitement de millions de transactions relatives aux prestations afin de répondre aux besoins des canadiens. De façon continue, EDSC soutient plus de 400 applications de GI-TI pour offrir des prestations dont dépendent des millions de canadiens, dont plus de 100 permettent des services essentiels. Cette complexité entraîne des problèmes d'exactitude des rapports et des données ainsi que de la difficulté à déterminer l'état de préparation d'EDSC (p. ex., exercice de surveillance et achèvement du plan d'urgence).

La consolidation de l'information et des données sur la gestion des urgences d'EDSC (c.-à-d. une base de données relationnelle) augmentera la confiance d'EDSC dans la prise de décisions lors de situations d'urgence en améliorant les capacités de surveillance (p. ex., l'achèvement du plan), l'identification des interdépendances (p. ex., entre les programmes, les services, les systèmes de TI et leurs emplacements géographiques) et l'information et les données à jour.

EDSC a besoin d'accéder à l'information et aux données d'urgence, via SAGU, pour coordonner et intervenir lors de situations d'urgence dans ses secteurs d'activité et de sa zone géographique. Pour ce faire, EDSC a besoin d'un système accessible à l'échelle du Canada qui assure une résilience contre les pannes de réseau.

La coordination et la surveillance de la préparation aux situations d'urgence d'EDSC (p. ex., achèvement du plan d'urgence et des exercices) font face aux mêmes défis liés à la répartition de l'effectif mentionnés ci-dessus. EDSC a besoin d'un système qui facilite la surveillance et le partage de l'information ainsi que la création de plans et de rapports normalisés à l'échelle du ministère.

2. But et priorités

Le SAGU vise à simplifier les quatre secteurs fonctionnels de la gestion des urgences à EDSC en tenant compte des priorités suivantes :

- Disponibilité
- Automatisation
- Surveillance

- Exactitude des données
- Protection du personnel, des biens et des opérations en cas d'urgence.

Les principaux facteurs de réussite sont la préparation (p. ex. planification, mise à l'essai et surveillance) de la continuité des activités et de la reprise des services de TI ainsi que l'efficacité de la coordination et de la communication entre les nombreux intervenants dans la coordination d'une intervention ministérielle, régionale et locale en cas d'urgence.

État actuel

Présentement, les solutions déployées à EDSC offrant des fonctionnalités semblables à celles requises par le SAGU sont disparates, ne partagent pas l'information entre elles et ne sont que partiellement automatisées. Plusieurs de ces outils se sont révélés efficaces, mais ne répondent pas entièrement à tous les besoins d'EDSC. En remplacement, le SAGU nécessitera la migration des ressources d'information du système actuel.

3. Buts et objectifs

L'objectif du SAGU est de fournir aux utilisateurs d'EDSC à l'échelle du Canada un accès via une connexion Internet à un seul système automatisé qui gère les quatre piliers de la gestion des urgences.

Le SAGU a pour but d'améliorer la capacité d'EDSC à maintenir la sûreté et la sécurité de ses employés et de ses clients, de continuer à offrir les programmes et services d'EDSC aux canadiens lors de situation d'urgence et de s'acquitter de ses responsabilités en vertu du Plan fédéral d'intervention d'urgence soutenant les canadiens lors d'urgence fédérale.

4. Échéancier de mise en œuvre du projet

Le SAGU sera implanté en deux phases :

- Phase 1 : Fournir un accès initial à 20 utilisateurs principaux, une formation complète, la configuration des solutions/services, la migration des données existantes, la mise à l'essai et l'acceptation des services par le Canada.

  Les utilisateurs principaux sont ceux qui seraient en mesure de former les autres futurs utilisateurs et de participer activement à la configuration/installation, aux tests et à la migration des actifs d'information de la solution.

- Phase 2 : Accès aux 2 980 autres utilisateurs, leur formation et déploiement complet.

5. Portée

Le SAGU sera livré comme logiciel en tant que service (SaaS) qui répond le mieux à toutes les exigences énoncées dans le présent énoncé des besoins, y compris une conformité obligatoire aux contrôles de sécurité des technologies de l'information sélectionnés dans le document « *Profil de contrôle de sécurité du Canada pour les services de TI en nuage pour les niveaux Protégé B, Intégrité et disponibilité moyennes*

(PBMM) » ci-joint. Il sera livré dans le nuage public et aura la capacité de traiter les données Protégé B. Pour en savoir plus sur la conformité à la sécurité des TI et le raisonnement justifiant la sélection des contrôles, consultez le diagramme des modèles de services informatiques en nuage à l'annexe C.

La portée du présent approvisionnement englobe :

- Le SAGU, en tant que type de service SaaS; et
- Les services professionnels requis pour les aspects susmentionnés de la mise en œuvre et du déploiement.

La portée fonctionnelle du SAGU comprendra les éléments suivants :

1. Gestion de crise
2. Gestion de la continuité des activités
3. Planification de la reprise après sinistre
4. Planification de la reprise de la TI
5. Préparation aux situations d'urgence dans les immeubles
6. Essais et exercices
7. Communications d'urgence
8. Surveillance et production de rapports

Pour faciliter l'exécution du projet, le Canada exige que le soumissionnaire offre les services professionnels suivants :

1. Service de formation (approche de formation des formateurs)
   Le Canada exige que le soumissionnaire retenu offre une formation suffisamment complète aux vingt premiers utilisateurs (considérés comme des utilisateurs principaux) d'EDSC, pour leur permettre d'exécuter des fonctions administratives, c.-à-d. configuration, migration des actifs informationnels existants, mise à l'essai, formation et déploiement des services auprès des 2 980 autres utilisateurs.

2. Services de configuration et de mise à l'essai
   Le Canada exige que le soumissionnaire retenu fournisse des services professionnels pour la configuration, l'adaptation et la mise à l'essai du SAGU.

3. Services de migration
   Le Canada exige que le soumissionnaire retenu fournisse des services professionnels pour la migration des ressources d'information du Canada des anciens systèmes au SAGU.

4. Services de déploiement

   Le Canada exige que le soumissionnaire retenu fournisse des services professionnels pour le déploiement du SAGU aux 2 980 autres utilisateurs.

6. Rôles du SAGU

Le système du SAGU servira quatre (4) principaux types de rôles, qui auront les capacités respectives suivantes :

1. **Administrateur du SAGU** – dispose de tous les droits et privilèges :
   a. incluant les sous-rôles de responsable et d'approbateur du plan;
   b. configure et gère les paramètres du système;
   c. gère l'accès au système pour les utilisateurs d'EDSC;
   d. crée, gère et supprime l'information, les données et les flux de travail;
   e. produit des rapports et effectue une surveillance à l'échelle du système; et
2. **Coordonnateur du SAGU** – ses privilèges d'accès au système sont limités selon son secteur d'activité :
   a. gère l'accès au système pour les utilisateurs d'EDSC dans un secteur opérationnel donné;
   b. tient à jour les écrans du SAGU pour son secteur d'activité;
   c. crée, gère et supprime l'information, les données et les flux de travail;
   d. produit des rapports et effectue un suivi pour son secteur d'activité.
3. **Contributeur du SAGU** – ses privilèges d'accès au système sont limités selon son secteur d'activité :
   a. crée, modifie, gère et approuve les données, l'information et les flux de travail; et
   b. produit des rapports et effectue un suivi pour son secteur d'activité.
4. **Visualiseur du SAGU** – dispose de privilèges d'accès au système en mode lecture-seulement et restreints en fonction du domaine d'activité ou du besoin de savoir :
   a. dispose seulement des droits de visionnement; et,
   b. inclue un sous-rôle d'un membre du groupe de surveillance.

Les quatre types d'utilisateurs d'EDSC susmentionnés seront des représentants de divers secteurs, mais sans s'y limiter :

- Cadres d'EDSC
- Personnel d'urgence de l'immeuble
- Personnel du Centre national et des Centres régionaux des opérations d'urgence (CNOU)/(CROU)
- Bureaux régionaux de la sécurité

- Personnel de la gestion des incidents de TI
- Personnel de la santé et sécurité au travail
- Coordonnateurs de la continuité des activités et de la gestion des urgences

Les acronymes et les termes utilisés dans le présent document figurent aux Annexes A et B.

7. Exigences du SAGU

7.1. Exigences obligatoires

7.1.1. Exigences relatives à la conformité de la sécurité

Les exigences de sécurité suivantes (M1-M20) doivent être respectées afin de démontrer la conformité à la sécurité des données jusqu'au niveau Protégé B.

Le soumissionnaire peut décider d'indiquer si les fournisseurs de sa solution SaaS de PaaS et d'IaaS ont déjà obtenu le statut d'un fournisseur de ces services infonuagiques au Canada, comprenant le niveau Protégé B (un accord-cadre, communément appelé « DF infonuagique du GC »). Dans un tel cas, joint à la proposition, le soumissionnaire doit présenter des preuves respectives obtenues des fournisseurs d'IaaS et de PaaS.

Pour simplifier les réponses au tableau 1 ci-dessous, lorsqu'une exigence est liée à une PaaS ou à une IaaS, le soumissionnaire peut simplement indiquer la référence au « DF infonuagique du GC » si ce DF couvre ce qui est inclus dans l'exigence. Autrement, si le fournisseur de PaaS et d'IaaS du soumissionnaire n'a pas de « DF infonuagique du GC », la réponse doit être détaillée, comme le décrit le tableau.

Pour une composante de SaaS de l'une ou l'autre des exigences de sécurité ci-dessous, le soumissionnaire doit démontrer sa conformité détaillée comme décrit dans le tableau.

Tableau 1. Exigences relatives à la conformité en matière de sécurité (données jusqu'au niveau Protégé B)

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
MS1	**Assurance de tiers – Certifications et rapports** Le soumissionnaire et tous les fournisseurs qui fournissent des composants de logiciel en tant que service (SaaS) disponibles sur le marché dans le cadre de la solution du soumissionnaire doivent se conformer aux exigences de sécurité sélectionnées dans le Profil de contrôle de sécurité du gouvernement du Canada pour les services de TI en nuage du gouvernement du Canada à la date de clôture des soumissions. Pour chaque composante du SaaS disponible sur le marché qui est comprise dans la solution du soumissionnaire, le soumissionnaire et les fournisseurs, le cas échéant, doivent posséder les certifications de l'industrie suivantes pour démontrer leur conformité : • Norme ISO/CEI 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences; et • Norme ISO/CEI 27017:2015 Technologies de l'information – Techniques de sécurité – Code de pratique des contrôles de sécurité de l'information fondé sur ISO/CEI 27002 pour les services du nuage; et • ISO/IEC 27018:2019 Techniques de sécurité – Code de pratique pour la protection des renseignements personnels identifiables dans les nuages publics agissant comme processeurs de renseignements personnels identifiables; et • Rapport de Contrôle de l'organisation des services de l'AICPA (American Institute of	Le soumissionnaire doit fournir la preuve des certifications de l'industrie suivantes : i. ISO/IEC 27001:2013 ii. ISO/CEI 27017:2015 iii. ISO/CEI 27018:2019 iv. Contrôle de l'organisme de services de l'AICPA (SOC) 2 Type II Chaque certification doit : i. Être valide à la date de soumission; ii. indiquer la dénomination sociale du sous-traitant proposé; iii. Indiquer la date de la certification actuelle; iv. Indiquer la liste des actifs, de l'infrastructure de l'entrepreneur et des lieux de service visés par le rapport de certification; v. Être émise par un tiers indépendant qualifié en vertu de l'AICPA ou de CPA Canada et/ou du régime de certification ISO et conforme à la norme de système qualité ISO/IEC 17020. Le soumissionnaire doit également fournir les rapports de vérification connexes. Ces rapports de vérification doivent avoir été produits dans les 12 mois précédant le début du contrat proposé. La portée des rapports doit correspondre aux emplacements et aux services offerts par le SaaS proposé disponible sur le marché. Si la méthode découpée est utilisée pour exclure les organisations de sous-services	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	Certified Public Accountants) (SOC) 2 Type II pour les principes de confiance en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité.	comme l'hébergement de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être inclus. Le rapport doit provenir d'un tiers indépendant qualifié en vertu du régime de certification de l'AICPA ou de CPA Canada et/ou ISO et conforme à la norme de système qualité ISO/IEC 17020. En plus des exigences obligatoires précisées ci-dessus, le soumissionnaire peut fournir des preuves supplémentaires tirées des plans de sécurité du système, de la conception des systèmes d'information, de l'architecture du système d'information ou des documents qui fournissent une description complète du système qui démontrent la conformité avec le profil de contrôle de sécurité du GC pour les services de TI nuage du GC pour PBMM. Pour tout fournisseur qui a complété le processus d'évaluation de la PSC-STI, le soumissionnaire doit fournir des documents confirmant que le fournisseur a complété le processus d'intégration avec (i) une copie du plus récent rapport d'évaluation rempli et fourni par le gouvernement du Canada et (ii) une copie du plus récent rapport sommaire fourni par le gouvernement du Canada.	
MS2	**Rôles et responsabilités pour la sécurité** Le soumissionnaire doit avoir clairement défini les rôles et responsabilités liés aux contrôles de sécurité et aux caractéristiques des services entre le soumissionnaire, ses sous-traitants et le Canada dans la chaîne d'approvisionnement de la solution infonuagique proposée et du Canada.	Les rôles et responsabilités du soumissionnaire pour : i. la gestion de comptes; ii. la protection des frontières; iii. la sauvegarde des actifs et des systèmes d'information; iv. la gestion des incidents; v. la surveillance du système; et,	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
		vi. la gestion des vulnérabilités. Une liste contenant des renseignements sur les tiers (p. ex. filiales, sous-traitants, etc.) qui font partie de sa solution. Aux fins de la présente exigence, un fournisseur qui n'est qu'un fournisseur de biens pour le soumissionnaire, mais qui n'exécute aucune partie de la chaîne d'approvisionnement n'est pas considéré comme un tiers.	
MS3	**Isolement de la protection des données** La solution proposée doit isoler les données au Canada dans un centre de données approuvé. Aux fins de la présente demande de soumissions, un centre de données approuvé est défini comme suit : i. Un centre de données géographiquement situé au Canada; et ii. Un centre de données qui satisfait à toutes les exigences de sécurité et à toutes les certifications identifiées. Exigences relatives aux installations du centre de données : La solution proposée doit garantir que des mesures de sécurité sont mises en œuvre pour protéger les installations de TI et les actifs du système d'information sur lesquels les données du Canada sont stockées et traitées contre toutes les formes de falsification, de perte, de dommage et de saisie, et qui est basé sur une approche de prévention-détection-intervention-reprise de la sécurité physique. Les mesures de protection physique doivent être appliquées conformément aux contrôles de sécurité de la protection physique et de	La documentation du système ou la documentation technique qui décrit en détails les mesures de sécurité, notamment les politiques, les processus et les procédures qui sont mis en œuvre pour protéger les installations de TI et les actifs du système d'information sur lesquels les données du gouvernement du Canada sont stockées et traitées contre toutes formes de falsification, de perte, de dommage et de saisie, et qui est basé sur une approche de prévention-détection-intervention-reprise de la sécurité physique.	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	l'environnement (PE), de la maintenance (MA) et de la protection des médias (MP) décrits dans le ITSG-33 Profil des mesures de sécurité pour les services informatiques du gouvernement du Canada fondés sur le nuage pour PBMM et la mise en pratique des directives et des normes sur la sécurité physique de la Gendarmerie royale du Canada (GRC). Il s'agit à tout le moins des éléments suivants : i. capacités de redondance et de récupération suffisantes au sein et dans ses installations informatiques, géographiquement disparates et de sorte que la perte d'un centre de données n'empêche pas la récupération des données dans l'entente concernant le niveau de service prescrit; ii. gestion appropriée des supports informatiques; iii. maintenance contrôlée des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité en continue; iv. accès contrôlé aux périphériques de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; v. limiter l'accès physique aux actifs des systèmes d'information aux employés et aux contracteurs autorisés en fonction de leur poste ou de leur rôle et au principe du besoin de savoir, qui est validé par deux formes d'identification; vi. escorter les visiteurs et surveiller leur activité; vii. maintenir un registre d'accès physique; viii. contrôler et gérer les dispositifs d'accès physique; ix. mettre en application les mesures de protection des données du gouvernement du Canada dans		

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	d'autres sites de travail alternatifs (p. ex., lieux de télétravail); et, x. enregistrer et surveiller tout accès physique aux centres de données et tout accès logique aux composants des systèmes d'information qui hébergent les données du Canada, en combinant les registres d'accès et la vidéosurveillance dans toutes les zones délicates et des mécanismes de détection des intrusions.		
MS4	**Séparation des données** La solution proposée doit comprendre des contrôles visant à assurer une isolation appropriée des ressources de manière à ce que les ressources d'information ne soient pas amalgamées avec des données d'autres locataires pendant leur utilisation, leur stockage ou leur transit, et dans tous les aspects de la solution du soumissionnaire et de la fonctionnalité et de l'administration du système de l'infrastructure. Cela comprend la mise en place de contrôles d'accès et l'application d'une séparation logique ou physique appropriée pour soutenir : i. La séparation entre l'administration interne du soumissionnaire et les ressources utilisées par ses clients; et ii. La séparation des ressources des clients dans des environnements à locataires multiples afin d'empêcher un consommateur malveillant ou compromis d'avoir des conséquences sur le service ou les données d'un autre.	Documents démontrant comment le soumissionnaire se conforme aux exigences.	
MS5	**Protection des données**	Respectivement pour les deux premiers éléments énumérés :	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	La solution proposée doit permettre au gouvernement du Canada de stocker et de protéger ses données inactives, notamment les données sauvegardées ou conservées à des fins de redondance dans les limites géographiques du Canada. Ceci inclus : i. identifier et fournir au gouvernement du Canada une liste à jour des emplacements physiques, comprenant la ville, où peut se trouver les données canadiennes au Canada pour chaque centre de données qui sera utilisé pour fournir les services. identifier quelles parties des services sont fournies à partir de l'extérieur du Canada, y compris tous les emplacements où les données sont stockées et traitées et d'où ils gèrent le service. ii. s'assurer qu'il soit impossible de trouver des données précises sur un client dans nos médias sur les supports physiques; et iii. utiliser le cryptage pour s'assurer qu'aucune donnée n'est inscrite sur un disque non-encrypté.	i. Des captures d'écran du centre de données disponible où les centres de données canadiens figurent sur la liste des disponibilités; et ii. Une liste ou carte indiquant l'emplacement géographique des centres de données au Canada.	
MS6	**Installations du centre des données** La solution proposée doit inclure des mesures de sécurité pour la protection des installations de TI, les données et les actifs du système d'information sur lequel les données du Canada sont stockées et traitées contre toutes formes de falsification, de perte, de dommage et de saisie, qui est basée sur un système de prévention, de détection, d'intervention et de reprise de la sécurité matérielle. Les mesures de protection physique doivent être appliquées conformément ou	La documentation sur le système ou la documentation technique décrivant en détail les mesures de sécurité, notamment les politiques, les processus et les procédures, qui sont mis en œuvre pour protéger les installations de TI, les données et les biens des systèmes d'information dans lesquels les données du Canada sont stockées et traitées contre toute forme de falsification, de perte, de dommage et de saisie. Ces mesures reposent sur une approche de prévention, de détection, d'intervention et de reprise de la sécurité matérielle.	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	utiliser une approche adéquate axée sur le risque et harmonisée aux contrôles de sécurité physique et aux pratiques de la Norme opérationnelle sur la sécurité matérielle du Conseil du Trésor (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12329). Les mesures de sécurité requises en vertu de cette norme comprennent, à tout le moins, ce qui suit : i. capacités suffisantes de redondance et de récupération des données dans ses installations de TI et entre celles-ci. Elles doivent être géographiquement disparates, de sorte que la perte d'un centre de données n'empêche pas la récupération des données dans l'entente concernant le niveau de service prescrit; ii. manipulation appropriée des supports de TI; iii. maintenance contrôlée des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; iv. accès contrôlé aux périphériques de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; v. accès physique limité aux actifs des systèmes d'information aux employés et aux répondants autorisés en fonction de leur poste ou de leur rôle et du principe besoin de savoir et qui est validé par deux formes d'identification; vi. escorter les visiteurs et surveiller leur activité; vii. maintenir un registre d'accès physique; viii. contrôler et gérer les dispositifs d'accès physique; ix. mettre en application les mesures de protection des données du gouvernement du Canada dans		

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	d'autres sites de travail alternatifs (p. ex., lieux de télétravail); et, x. enregistrer et surveiller tout accès physique aux centres de données et de tout accès logique aux composants des systèmes d'information qui hébergent les données du Canada, en combinant les registres d'accès et la vidéosurveillance dans toutes les zones délicates et les mécanismes de détection des intrusions.		
MS7	**Respect de la vie privée dès la conception** La solution proposée doit : iii. Comprendre un cycle de développement de logiciels conforme à la norme ISO 27032 et intégrant la protection de la vie privée dès la conception; iv. se conformer au Cadre de gestion de la protection des renseignements personnels et aux exigences précisées dans la Norme ISO 29100; et v. Respecter les sept principes fondamentaux de la protection de la vie privée dès la conception (voir https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).	Description du cycle de développement des logiciels du soumissionnaire Une description du cadre de gestion de la protection des renseignements personnels du soumissionnaire, y compris les principes régissant la protection des renseignements personnels et un aperçu des politiques de protection des renseignements personnels du soumissionnaire	
MS8	**Gestion de l'accès** La solution proposée doit satisfaire aux exigences de sécurité suivantes en matière de gestion de l'accès : i. Gérer et surveiller l'accès à la solution, y compris à l'infrastructure sous-jacente, pour s'assurer que toutes les interfaces de service dans un	Documentation du système ou livre blanc décrivant les politiques, les processus et les procédures utilisés pour gérer la gestion de l'accès.	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	environnement multi locataire sont protégées contre l'accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC; ii. Restreindre et minimiser l'accès aux services et aux actifs d'information du Canada aux seuls dispositifs autorisés et aux utilisateurs finaux qui ont explicitement besoin d'y avoir accès; iii. Appliquer et vérifier les autorisations d'accès aux services et aux actifs d'information; iv. Limiter les accès aux interfaces de service qui hébergent les actifs et les actifs d'information uniquement aux utilisateurs identifiés, authentifiés et autorisés, ainsi qu'aux dispositifs et aux processus (ou services); v. Mettre en œuvre des politiques sur les mots de passe afin de protéger les informations d'identification contre toute compromission d'attaques en ligne ou hors ligne et pour détecter ces attaques en enregistrant et en surveillant des événements comme (i) l'utilisation réussie des informations d'identité (ii) l'utilisation inhabituelle des informations d'identité et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément à la norme ITSP 30.031 V2 (ou versions subséquentes) du CST (https://www.cse-cst.gc.ca/fr/node/1842/html/26717); vi. Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux (niveau 2 seulement) avec accès, conformément à la politique ITSP.30.031 V2 (ou versions subséquentes) du CST (https://www.cse-cst.gc.ca/fr/node/1842/html/26717); vii. Mettre en œuvre des mécanismes de contrôle de l'accès fondés sur les rôles pour attribuer des		

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	privilèges qui constituent la base de l'application de l'accès aux actifs et aux actifs d'information; viii. Définir et mettre en œuvre la séparation des tâches pour atteindre, au minimum, la séparation des rôles de gestion des services et d'administration des rôles de support du système d'information, des rôles de développement des rôles opérationnels et des rôles de gestion des accès à d'autres rôles opérationnels; ix. Respecter les principes du droit d'accès minimal et du besoin de savoir au moment de donner accès aux services et aux actifs, et aux actifs d'information; x. Mettre en place des contrôles d'accès aux objets stockés et politiques d'autorisation granulaires pour autoriser ou limiter l'accès xi. Utiliser des points d'extrémité renforcés par la sécurité (p. ex., ordinateurs, appareils d'utilisateur final, serveurs intermédiaires, etc.) configurés pour une fonctionnalité minimale (p. ex., point d'extrémité dédié qui n'offre pas de navigation sur Internet ou d'accès ouvert à la messagerie) pour assurer le soutien et l'administration des Services et Infrastructure de l'entrepreneur; xii. Mettre en œuvre un processus automatisé pour vérifier périodiquement, au minimum, les actions de création, de modification, d'activation, de désactivation et de suppression de comptes; et xiii. Au moment de la cessation d'emploi, résilier ou révoquer les informations d'authentification et d'accès associés à tout membre du personnel.		
MS9	**Fédération de l'identité**	La documentation du système ou la documentation technique décrivant et détaillant les mesures de sécurité, y	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	La solution proposée doit appuyer l'intégration de l'identité fédérée, notamment : i. Mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs au moyen d'un accès privilégié, conformément à la politique ITSP.30.031 V2 du CST (ou versions subséquentes) (https://www.cse-cst.gc.ca/fr/node/1842/html/26717); ii. Le soutien du langage de balisage des assertions de sécurité (SAML) 2.0 et l'OpenID Connect 1.0 où les justificatifs d'identité et l'authentification de l'utilisateur final aux services infonuagiques sont sous le contrôle exclusif du Canada; et iii. La capacité d'associer des identifiants uniques au Canada (p. ex., un identifiant unique au Canada, une adresse électronique au Canada, etc.) avec le ou les compte(s) d'utilisateur de service informatique en nuage correspondants.	compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité.	
MS10	**Protection des points d'extrémité** La solution proposée doit comprendre la mise en œuvre, la gestion et la surveillance des points d'extrémité a sécurité renforcée afin de prévenir les attaques et abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du NIST 800-123 (Guide to General Server Security), le Center for Internet (CIS) ou une norme équivalente approuvée par écrit par le Canada.	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection des points d'extrémité.	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
MS11	**Développement sécurisé** La solution proposée doit comprendre la mise en œuvre d'un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de sécurité des systèmes d'information tout au long du cycle de vie du système d'information et lors du développement de logiciels, de sites Web et de services, et qui est conforme aux normes et aux pratiques exemplaires de l'industrie, notamment : i. NIST ii. ASI iii. ITSG-33 iv. SAFECode ou v. Normes de l'Open Web Application Security Project (OWASP) telles que l'Application Security Verification Standard (ASVS) ou une norme équivalente approuvée par écrit par le Canada.	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en place pour le développement sécurisé.	
MS12	**Gestion à distance de l'entrepreneur** La solution proposée doit être en mesure de gérer et de surveiller l'administration à distance de la solution du soumissionnaire qui sert à héberger les services du gouvernement du Canada et de prendre des mesures raisonnables pour : i. Mettre en œuvre des mécanismes d'authentification multi facteur pour authentifier les utilisateurs d'accès à distance, conformément à la politique ITSP.30.031 V2 du CST (ou versions subséquentes)	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la gestion à distance de l'entrepreneur	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	(https://www.cse-cst.gc.ca/fr/node/1842/html/26717); ii. Utiliser des mécanismes cryptographiques approuvés par le Centre de la sécurité des télécommunications du Canada pour protéger la confidentialité des sessions d'accès à distance; iii. Acheminer tous les accès à distance par des points de contrôle d'accès contrôlés, surveillés et vérifiés; iv. Débrancher ou désactiver rapidement les connexions non autorisées de gestion ou d'accès à distance; v. Autoriser l'exécution à distance des commandes privilégiées et l'accès à distance des informations relatives à la sécurité.		
MS13	**Fuite d'information** Le processus proposé en cas d'incident de fuite d'information doit être harmonisé avec le guide ITSG-33, Contrôle de sécurité pour l'intervention en cas de fuite d'information IR-9.	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, les processus et les procédures qui sont mis en œuvre pour la protection contre la fuite d'information.	
MS14	**Protection cryptographique** La solution proposée doit : i. Configurer toute cryptographie utilisée pour mettre en œuvre des mesures de protection de la confidentialité ou de l'intégrité ou utilisée dans le cadre d'un mécanisme d'authentification (p. ex., solutions RPV, TLS, modules logiciels, ICP et jetons d'authentification, le cas échéant), conformément aux algorithmes cryptographiques approuvés par le	Documentation du système ou documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour assurer la protection cryptographique	

Numéro	Critère	Obligation d'information du soumissionnaire	Renvoi à la proposition du soumissionnaire
	Centre de la sécurité des télécommunications (CST) ainsi qu'aux tailles et périodes cryptographiques des clés cryptographiques; ii. Utiliser des algorithmes cryptographiques ainsi que des tailles de clés cryptographiques et des périodes cryptographiques qui ont été validés par le Programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/ - en anglais seulement) et qui sont précisés dans le document ITSP.40.111, Algorithmes cryptographiques pour les renseignements non classifiés, Protégé A et Protégé B, ou les versions subséquentes (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b); iii. S'assurer que la cryptographie validée selon la norme FIPS 140 est utilisée lorsque le chiffrement est requis et qu'elle est mise en œuvre, configurée et exploitée dans un module cryptographique validé par le Programme de validation des modules cryptographiques (https://www.cse-cst.gc.ca/fr/group-groupe/crypto-module-validation-program) en mode approuvé ou autorisé afin d'assurer un degré élevé de certitude que le module cryptographique validé selon la norme FIPS 140-2 fournit les services de sécurité attendus de la manière prévue; et iv. S'assurer que tous les modules FIPS 140-2 utilisés sont certifiés actifs, à jour et valides. Les produits conformes à la norme FIPS 140 auront des numéros de certificat.		

7.1.2 Exigences fonctionnelles – Obligatoires

Tableau 2 – Exigences fonctionnelles obligatoires

ID	Exigence	Justification
M1	Le système proposé par le soumissionnaire doit être une solution infonuagique de logiciel en tant que service (SaaS).	Le soumissionnaire doit démontrer sa conformité au moyen de documents techniques et d'autres moyens de preuve, comme la saisie d'écran.
M2	Le système logiciel proposé par le soumissionnaire doit être fonctionnel de façon équivalente dans les deux langues officielles du Canada (anglais et français) et doit permettre aux utilisateurs de travailler dans la langue officielle canadienne de leur choix.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M3	Le système proposé par le soumissionnaire doit permettre un accès simultané par 2 000 utilisateurs d'EDSC.	Le soumissionnaire doit démontrer sa conformité en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final qui démontrent clairement cette capacité.
M4	Le système proposé par le soumissionnaire doit pouvoir prendre en charge au moins 3 000 utilisateurs d'EDSC.	Le soumissionnaire doit démontrer sa conformité en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final qui démontrent clairement cette capacité.
M5	Le système proposé par le soumissionnaire doit fournir une capacité de gestion des documents et de l'information électroniques (p. ex., stockage, recherche, extraction et gestion des documents), organisée de manière hiérarchique (p. ex., par région, direction générale, direction).	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M6	Le système proposé par le soumissionnaire doit offrir une capacité dans toutes les catégories suivantes : 1. Gestion de la continuité des activités; 2. Gestion de la reprise de la TI; 3. Gestion des urgences et évacuations des immeubles (équipes et plans d'urgences de l'immeuble); 4. Gestion des urgences; 5. Gestion de crise;	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Justification
M7	Le système proposé par le soumissionnaire doit permettre la création, la gestion et l'approbation de plans de continuité des activités (PCA) intégrés pour les services au niveau ministériel, ce qui comprend le cumul des plans de continuité des activités à plusieurs niveaux organisationnels d'EDSC (p. ex., PCA au niveau régional, au niveau des directions générales, des directions et des divisions).	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M8	Le système proposé par le soumissionnaire doit être disponible : 1. À l'échelle du Canada 2. À l'aide d'une connexion à un réseau câblé et sans fil; et 3. Par le biais d'un ordinateur de bureau et d'appareils mobiles (p. ex., par le biais d'un navigateur Web mobile ou d'une application mobile)	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M9	Le système proposé par le soumissionnaire doit permettre de créer, de modifier, de remplir, d'enregistrer et de gérer des questionnaires (p. ex., questionnaire d'analyse des répercussions sur les activités) et des listes de vérification.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M10	Le système proposé par le soumissionnaire doit fournir une capacité de gestion du flux de travail, notamment : 1. Permettre aux utilisateurs du SAGU : i. de créer, assigner, réassigner et supprimer des tâches de flux de travail, ii. de créer, démarrer, retirer, supprimer, compléter les flux de travail, iii. de visualiser les flux et les tâches actifs, iv. d'établir des délais de présentation des flux de travail (ponctuels ou planifiés) pour toute tâche; et v. de surveiller les flux de travail et d'en produire des rapports. 2. Exécuter automatiquement des flux de travail des documents électroniques	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Justification
M11	Le système proposé par le soumissionnaire doit offrir aux administrateurs du SAGU et aux coordonnateurs du SAGU la capacité de gérer le contrôle de l'accès des utilisateurs (y compris la protection des renseignements personnels) et les paramètres d'autorisation.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M12	Les paramètres de confidentialité du système proposés par le soumissionnaire doivent permettre de restreindre la consultation des données sur les employés, selon la structure organisationnelle (c.-à-d. que les gestionnaires ne devraient voir que les données sur les employés des personnes affectées à leur unité de travail).	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M13	Le système proposé par le soumissionnaire doit offrir une capacité de production de rapports qui comprend tous les éléments suivants : 1. Création de rapports spéciaux en extrayant des données de n'importe quel champ de base de données. 2. 3. Personnalisation des rapports 3. 2. Création et gestion de modèles de rapports (retrait, modification et suppression) 4. Création de rapports programmés	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M14	Le système proposé par le soumissionnaire doit permettre de produire des documents et des rapports électroniques imprimables.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M15	Le système proposé par le soumissionnaire doit sauvegarder quotidiennement tous les justificatifs d'identité, données et fichiers des utilisateurs d'EDSC (p. ex., rapports de vérification, documents, listes de personnes-ressources) dans un système de sauvegarde stocké dans un centre de données situé à un endroit différent du centre de données principal. Le centre de données secondaire doit être situé au Canada.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Justification
M16	Le système proposé par le soumissionnaire doit satisfaire à la Norme de l'UE (EN 301 549), sections 5, 7, 9 et 12	Le soumissionnaire doit démontrer sa conformité en incluant à sa soumission une évaluation officielle de la conformité, par exemple, dans l'ordre de préférence du Canada : – Rapport de conformité à l'accessibilité (RCA) d'un évaluateur tiers accrédité. – Modèle d'accessibilité volontaire des produits (VPAT) par un évaluateur tiers accrédité. – VPAT, autoévalué. Remarque : Dans la norme de l'UE, certaines des sections sélectionnées font référence à la norme WCAG 2.1. Le soumissionnaire peut compléter sa justification en fournissant toute autre preuve, capture d'écran ou documentation technique, acceptée par l'industrie.
M17	Le système proposé par le soumissionnaire doit permettre de fournir des avis aux utilisateurs avant d'accorder l'accès et doit permettre aux utilisateurs de configurer le message de notification selon leurs besoins.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.1.3 Exigences non fonctionnelles – obligatoires

Tableau 3 – Exigences non fonctionnelles obligatoires

ID	Exigence	Justification
M18	Le système proposé par le soumissionnaire doit permettre d'identifier et d'authentifier de façon unique les connexions à partir d'appareils externes et d'autoriser les appareils avant de permettre la connectivité.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M19	Le système proposé par le soumissionnaire doit afficher toutes les tentatives d'ouverture de session infructueuses depuis la dernière ouverture de session réussie.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M20	Le système proposé par le soumissionnaire doit permettre de mettre fin à une session d'utilisateur lorsqu'un utilisateur a procédé à une fermeture de session.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M21	Le système proposé par le soumissionnaire doit permettre d'indiquer clairement sur tout écran d'affichage, fichier, imprimé ou courriel qu'il contient des données correspondant aux niveaux de confidentialité suivants (voir le glossaire pour les définitions) : 1. Non classifié 2. Protégé A 3. Protégé B *consulter les définitions des niveaux de confidentialité dans le glossaire.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Justification
M22	Le soumissionnaire doit inclure dans sa soumission l'entente sur les niveaux de service publiée pour le système proposé. Les engagements de niveau de service inclus doivent fournir à EDSC des services de garantie, de maintenance et de soutien. Les services de soutien peuvent être fournis par téléphone, par courriel, par messagerie mobile ou par des outils Web, selon le cas.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M23	Le soutien du soumissionnaire doit permettre aux utilisateurs de signaler et de suivre les problèmes, en ligne ou par téléphone.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M24	Le soumissionnaire doit fournir la documentation qui décrit ses processus pour le système proposé : 1. Gestion de la configuration; 2. Gestion et contrôle du changement (p. ex., comme ITIL,Information Technology Infrastructure Library); et 3. Gestion des services.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M25	Le soumissionnaire doit s'assurer que toutes les données du SAGU seront accessibles au Canada, en format CSV, y compris le fichier de métadonnées, aux fins de rapatriement au Canada, dans les trois (3) mois suivant l'annulation de l'accès au système.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M26	Le soumissionnaire doit s'assurer que, sur demande du Canada, dans les cinq jours ouvrables, l'extrait de données du SAGU sera disponible au Canada, en format CSV, y compris le fichier de métadonnées, aux fins de rapatriement au Canada.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
M27	Le soumissionnaire doit fournir des services de soutien technique aux administrateurs du SAGU par téléphone, courriel, messagerie mobile ou outils Web, selon le cas.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de satisfaire aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'autres documents appropriés pour compléter sa réponse.

ID	Exigence	Justification
M28	La solution disponible sur le marché du soumissionnaire doit avoir la capacité, et le soumissionnaire doit être disposé, à la demande du Canada, à l'intégrer aux solutions demandées du marché pertinent ou aux systèmes sur place du Canada (p. ex., Microsoft Active Directory).	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2. Exigences cotées

Ce qui suit s'applique à toutes les exigences cotées : Dans leur réponse, les soumissionnaires doivent démontrer leur conformité en fournissant la documentation décrivant leur capacité de répondre à l'exigence. Le soumissionnaire peut fournir des captures d'écran et des documents techniques ou d'utilisateur pour compléter sa réponse.

7.2.1. Exigences fonctionnelles - Cotées

Les exigences de cette section sont regroupées selon les principales fonctionnalités requises dans le SAGU.

7.2.1.1 Gestion de la continuité des activités

ID	Exigence	Critères de notation	Justification
R1	Le système proposé par le soumissionnaire doit permettre aux utilisateurs d'EDSC de créer et de gérer les types suivants de documents de **gestion des urgences** (GU) : 1. Analyse des répercussions sur les activités 2. Plans de continuité des opérations 3. Plans d'urgence des immeubles 4. Plans de contingence 5. Plans de continuité des TI (p. ex. plan de reprise après sinistre) 6. Liste des applications essentielles 7. Listes de personnes-ressources 8. Évaluation de la vulnérabilité ou des menaces et des risques de l'immeuble 9. Liste de vérification des inspections d'étages 10. Rapports de situation	Chacun des éléments énumérés vaut 2 points, pour un total de 32 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	11. Plans d'action 12. Calendrier des activités de GU 13. Rapports après action (RAA) 14. Questionnaires 15. Rapports de conformité, p. ex., achèvement du plan de GU, conformité du personnel de secours de l'immeuble (par étage, par immeuble) 16. Listes de contrôle		
R2	Le système proposé par le soumissionnaire devrait être en mesure d'aider les utilisateurs d'EDSC à gérer les composantes suivantes du programme **Gestion de la continuité des activités** : 1. Cycles d'examen de la documentation 2. Évaluation des risques 3. Analyse des répercussions sur les activités 4. Plans d'intervention en cas d'incident 5. Plans de continuité des opérations 6. Plans de communication d'urgence 7. Documents de sensibilisation et de formation 8. Politiques et procédures 9. Plans de continuité des TI	Chacun des éléments énumérés vaut 3 points, pour un total de 27 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R3	Le système proposé par le soumissionnaire doit comprendre une capacité d'**analyse des répercussions sur les activités** qui comprend la capacité d'évaluer les types d'incidence suivants : 1. Incidence sur la santé des Canadiens/du public 2. Incidence sur la sûreté des Canadiens/du public 3. Incidence sur la sécurité des Canadiens/du public 4. Incidence sur le bien-être économique des Canadiens/du public 5. Incidence sur la fonction du gouvernement ou de l'organisation	Chacun des éléments énumérés vaut 4 points, pour un total de 28 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	6. Incidence sur la confiance et la réputation du public dans le Ministère ou l'organisation 7. Incidence sur la conformité juridique et réglementaire sur le Ministère ou l'organisation Voir l'Annexe B pour les définitions des types d'incidence énumérés.		
R4	Le système proposé par le soumissionnaire devrait (p. ex., en utilisant des modèles) permettre d'utiliser les ensembles de données existants pour faciliter la saisie de modèles personnalisables.	La convivialité de cette capacité est : 1. Facile pour les utilisateurs finaux et les administrateurs du SAGU – 30 points 2. Facile soit pour l'utilisateur final, soit pour l'administrateur du SAGU – 15 points 3. Pas facile pour tout type d'utilisateur – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R5	Le système proposé par le soumissionnaire doit permettre de créer des modèles (format, disposition et champs de données) pour chaque type de plan et de rapport de gestion des urgences (GU). Le système proposé devrait permettre à l'utilisateur : 1. D'inclure les champs de données définis par EDSC, notamment : i. Données de documents électroniques créés précédemment ii. Données entrées manuellement par les utilisateurs d'EDSC	Chacun des éléments énumérés vaut 2 points, pour un total de 20 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	iii. Données provenant d'ensembles de données publiques (p. ex., données des cartes de Google). iv. Toute donnée d'EDSC 2. De définir le format du document électronique connexe, notamment : i. Disposition (emplacement des champs) ii. En-têtes iii. Titre iv. Orientation des pages v. Tableaux vi. Figures		
R6	Le système proposé par le soumissionnaire devrait inclure un modèle de liste de personnes-ressources. Le modèle de liste de personnes-ressources doit être configurable pour permettre aux utilisateurs de saisir les données suivantes concernant la personne-ressource : 1. Nom 2. Titre 3. Structure organisationnelle à laquelle il appartient 4. Téléphone(s) cellulaire(s)/BlackBerry cellulaire/Télécopieur 5. Téléphone à la maison 6. Courriel interne et externe 7. Compétences ou capacité particulières (p. ex., réanimation cardiorespiratoire [RCR], premiers soins, accès à un RPV, rôle au sein du personnel d'urgence de l'immeuble) 8. Travail à l'extérieur des locaux 9. Emplacement (p. ex., immeuble) 10. Champs personnalisés	Chacun des éléments énumérés vaut 1 point, pour un total de 10 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2.1.2. Gestion de la continuité des activités

ID	Exigence	Critères de notation	Justification
R7	Le modèle d'analyse des répercussions sur les activités (ARA) proposé par le soumissionnaire doit être configurable pour saisir les données suivantes : 1. Fonctions et services opérationnels identifiés, 2. Objectifs de temps de reprise (y compris les dépendances de la TI), 3. Objectifs des points de reprise (y compris les dépendances en matière de TI), 4. Temps d'arrêt maximal admissible 5. Niveau de service normal 6. Niveau de service minimal 7. Répercussion des interruptions, 8. Temps de fonctionnement essentiel et de pointe, 9. Interdépendances en aval (p. ex., qui compte sur vous, interne par rapport à externe), 10. Interdépendances en amont (p. ex., de qui dépendez-vous?) 11. Dépendances de la technologie de l'information (p. ex., applications incluant types, systèmes, infrastructure) 12. Infrastructure essentielle (p. ex., infrastructure de réseautage, stockage, centre de données). 13. Exigences minimales en matière de ressources (p. ex., niveaux de dotation).	Chacun des éléments énumérés vaut 1 point, pour un total de 13 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R8	Le modèle de plan de continuité des activités (PCA) proposé par le soumissionnaire doit être configurable pour saisir les données suivantes : 1. Profil (description) 2. Plan de mise en œuvre du PCA 3. Liste de vérification pour la reprise 4. Stratégie de communication 5. Organigrammes pour l'équipe de gestion de crise 6. Fonctions ou services opérationnels essentiels et stratégies de reprise (notamment ODR, DIMA, ODR, interdépendances). 7. Fonctions ou services opérationnels non critiques 8. Multiples listes de personnes-ressources pour tout le personnel essentiel 9. Lieux de travail de remplacement (p. ex., sous-ministre, activités essentielles) 10. Structure organisationnelle configurable (p. ex., service, équipe d'évacuation d'urgence de l'immeuble) 11. Liste des personnes-ressources externes en cas d'urgence (p. ex., premiers intervenants). 12. Inventaire des équipements, biens et logiciels essentiels 13. Cartes et itinéraires pour les lieux des réunions d'urgence 14. Information locale et communautaire. 15. Journal des incidents et des interventions de l'équipe du PCA 16. Registre des documents du PCA 17. Documents essentiels (procédures opérationnelles normalisées – PON, procédures manuelles de rechange, dossiers papier).	Chacun des éléments énumérés vaut 1 point, pour un total de 17 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R9	Le système proposé par le soumissionnaire doit inclure la capacité d'élaborer des stratégies de reprise et leurs analyses coûts-avantages respectives.	Le système proposé par le soumissionnaire : 1. Appuie entièrement l'élaboration de stratégies de reprise fondées sur les données d'entrée, y compris l'analyse coûts-avantages – 10 points. 2. Appuie entièrement l'élaboration de stratégies de reprise fondées sur les données d'entrée, mais ne comprend pas l'analyse coûts-avantages connexe – 6 points. 3. Contient uniquement des champs de texte pour consigner les stratégies de reprise et les coûts connexes – 3 points. 4. N'appuie ni l'élaboration de stratégies de reprise ni l'analyse coûts-avantages – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R10	Le système proposé par le soumissionnaire doit satisfaire aux principales normes de gestion de la continuité des activités (GCA) suivantes : 1. ISO 22301 (Gestion de la continuité des activités) 2. ISO 27031 (reprise après sinistre des TI) 3. ISO 31000 Techniques de gestion du risque	Le système proposé par le soumissionnaire : 1. Satisfait à toutes les normes énumérées – 10 points 2. Satisfait à deux des normes énumérées – 6 points 3. Satisfait à l'une des normes énumérées – 3 points 4. Ne satisfait à aucune des normes énumérées – 0 point	Le soumissionnaire doit démontrer sa conformité en fournissant les certifications énumérées. Si le soumissionnaire est en voie d'obtenir ces certifications, il doit en fournir la preuve, à l'aide d'autres documents pertinents ou de saisies d'écran démontrant le fondement.

7.2.1.3. Gestion des urgences

ID	Exigence	Critères de notation	Justification
R11	Le plan d'urgence et d'évacuation de l'immeuble proposé par le soumissionnaire doit être configurable afin de permettre la saisie des données suivantes : 1. Coordonnées d'urgence (internes et externes). 2. Liste configurable de l'équipement et des systèmes et équipements d'urgence de l'immeuble. 3. Renseignements sur l'occupation (p. ex., population d'occupants, % d'occupation locataire principal/locataire secondaire) 4. Plans d'étage et dessins architecturaux 5. Renseignements sur l'immeuble (p. ex., ascenseurs, heures normales, alertes, hauteur et taille de l'immeuble) 6. Procédures d'urgence 7. Rôles et responsabilités du personnel d'urgence de l'immeuble 8. Personne-ressource 9. Registre des activités du personnel d'urgence de l'immeuble 10. Carte des lieux de rassemblement en cas d'urgence 11. Pièces jointes diverses (p. ex., registre des activités du personnel d'urgence de l'immeuble, organigrammes, copie du pompier) 12. Liste de vérification des vulnérabilités de l'immeuble 13. Partage de locaux (p. ex., autres ministères du Canada, organismes privés, etc.) 14. Liste du personnel d'urgnece de l'immeuble par étage	Chacun des éléments énumérés vaut 2 points, pour un total de 28 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R12	Le système proposé par le soumissionnaire devrait permettre aux utilisateurs d'EDSC de créer et de gérer des listes de vérification. Ces listes de vérification doivent contenir des données sur les éléments suivants : 1. Dangers en milieu de travail 2. Équipement d'intervention d'urgence 3. Équipement de santé et de sécurité 4. Équipes et personnel d'urgence 5. Formation	Chacun des éléments énumérés vaut 4 points, pour un total de 20 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2.1.4. Planification de la continuité de la TI

ID	Exigence	Critères de notation	Justification
R13	Le modèle du système proposé par le soumissionnaire pour le plan de continuité de la TI (ou plan de reprise après sinistre) doit être configurable pour saisir les données suivantes : 1. Buts et objectifs 2. Portée 3. Hypothèses et limites 4. Définitions 5. Rôles et responsabilités (p. ex., listes de personnes-ressources et équipes) 6. Aperçu du système – Nom du système, acronyme, ID 7. Aperçu de l'infrastructure de continuité de la TI (p. ex., diagrammes, listes, etc.) 8. Ententes sur les niveaux de service 9. Capacité d'évaluation des incidences (capacité d'établir des liens avec les services essentiels) 10. Procédure d'activation du plan (p. ex., mention des intervenants qui peuvent activer le plan)	Chacun des éléments énumérés vaut 1 point, pour un total de 24 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	11. Signalement de l'incident 12. Procédures de rétablissement 13. Validation du rétablissement 14. Procédures de traitement de secours 15. Processus de communication 16. Procédure de signalement aux échelons supérieurs 17. Considérations relatives à la sécurité de la TI 18. Piste de vérification des modifications apportées aux documents 19. Essais et exercices 20. Capacité d'exploiter les métadonnées du système, y compris les données de l'analyse des incidences sur les activités, les plans de continuité des activités, etc. 21. Objectif de délai de reprise des systèmes de TI 22. Objectif de point de reprise des systèmes de TI 23. Temps d'arrêt maximal admissible – pour les services opérationnels essentiels 24. Personne-ressource du programme de continuité de la TI d'EDSC		

7.2.1.5. Gestion de crise

ID	Exigence	Critères de notation	Justification
R14	Le système proposé par le soumissionnaire devrait être en mesure d'aider les utilisateurs d'EDSC à gérer les urgences et les incidents de TI et à en rendre compte au moyen des fonctions suivantes : 1. Création de l'incident 2. Notification de l'incident 3. Transmission des incidents aux paliers supérieurs 4. Gestion de l'incident 5. Fermeture de l'incident 6. Rapports sur l'incident 7. Création d'une liste de contrôle des mesures 8. Capacité de tirer parti d'autres sources de données d'EDSC, comme les plans de gestion des urgences.	Chacun des éléments énumérés vaut 4 points, pour un total de 32 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R15	Le modèle de plan d'action en cas d'incident du système proposé par le soumissionnaire doit être configurable pour saisir les données suivantes : 1. Type d'urgence 2. Heure du signalement 3. Objectif(s) 4. Stratégies pour l'atteinte des objectifs 5. Date/heure d'achèvement estimée 6. État au moment du signalement	Chacun des éléments énumérés vaut 5 points, pour un total de 30 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R16	Le système proposé par le soumissionnaire doit fournir une fonction de notification de masse en cas d'urgence, intégrée ou externe, capable de transmettre des messages d'urgence de masse ciblés par quatre canaux : 1. Courriel; 2. Messagerie instantanée; 3. Appareil mobile; et 4. Téléphone fixe.	Le système proposé par le soumissionnaire prend en charge un système d'avertissement de masse en cas d'urgence : 1. Entièrement, par l'entremise des quatre canaux énumérés et comprend des moyens d'identifier la transmission du message et la	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
		confirmation de réception. - 20 points 2. Par l'entremise d'au moins deux des canaux énumérés et comprend des moyens d'identifier la transmission du message et la confirmation de réception. - 15 points 3. Par l'un des canaux énumérés et comprend des moyens d'identifier la transmission du message et la confirmation de réception; OU par plus d'un des canaux énumérés, mais ne comprend pas de moyens d'identifier la livraison du message et la confirmation de la réception. - 10 points 4. Par l'un des canaux énumérés, mais ne comprend pas de moyens d'identifier la livraison du message et la confirmation de réception. – 5 points 5. Impossible de prendre en charge un système d'avertissement de masse en cas d'urgence – 0 point	
R17	Le système proposé par le soumissionnaire doit permettre aux utilisateurs d'EDSC d'envoyer des notifications (p. ex., préapprouvées ou spéciaux) aux utilisateurs d'EDSC par l'entremise des moyens suivants : 1. Courriel préapprouvé 2. Courriel spécial 3. Texte préapprouvé 4. Texte spécial	Chacun des éléments énumérés vaut 3 points, pour un total de 12 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R18	Le système proposé par le soumissionnaire devrait être en mesure de mettre à jour les champs de données d'EDSC contenus dans les notifications préapprouvées dans l'ensemble de données pertinent le plus récent avant d'envoyer des notifications préapprouvées. Ces champs permettent de saisir les données suivantes : 1. Date 2. Heure 3. Emplacement (c.-à-d. étage(s), immeuble, région) 4. Nom et type d'urgence 5. Mesures d'urgence	Chacun des éléments énumérés vaut 2 points, pour un total de 10 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2.1.6. Exercices

ID	Exigence	Critères de notation	Justification
R19	Le système proposé par le soumissionnaire doit permettre aux utilisateurs d'EDSC de planifier les activités de gestion des urgences (GU) suivantes : 1. Exercices de gestion de la continuité des activités 2. Exercices de GU 3. Exercices de continuité des activités de la TI 4. Cycles de création et d'examen des documents électroniques 5. Formation du personnel d'urgence des immeubles 6. Activités de sensibilisation à la GU	Chacun des éléments énumérés vaut 5 points, pour un total de 30 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R20	Le système proposé par le soumissionnaire, tout en planifiant les activités de gestion des urgences	Chacun des éléments énumérés vaut 2 points, pour un total de 12 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des

ID	Exigence	Critères de notation	Justification
	(GU), devrait permettre de saisir les données suivantes : 1. Direction générale/région 2. Type d'activité de GU 3. Jour, mois et année de l'activité de GU 4. Nom du responsable de l'activité de GU 5. Titre de l'activité de GU 6. Objectif de l'activité de GU		saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R21	Le système proposé par le soumissionnaire doit permettre de gérer et d'exécuter les types d'exercices de gestion des urgences suivants et d'en rendre compte : 1. Exercices axés sur la discussion (p. ex., revue générale) 2. Exercices pratiques (p. ex., confinement, évacuation, intrus actif) 3. Exercices de simulation (p. ex., opérationnels et fonctionnels) 4. Exercices à grande échelle 5. Continuité de la TI et reprise après sinistre	Chacun des éléments énumérés vaut 4 points, pour un total de 20 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R22	Le système proposé par le soumissionnaire doit permettre de créer et/ou de personnaliser des modèles, par exemple pour les types suivants de documentation d'**exercice** : Ordres du jour Liste chronologique des événements Fiche d'intrants Manuel de l'animateur Manuel du contrôleur Manuel de l'évaluateur Manuel des joueurs Guide de l'observateur Formulaire d'évaluation du participant Formulaire d'évaluation de l'observateur	Chacun des éléments énumérés vaut 1 point, pour un total de 15 points. Cette capacité du système proposé par le soumissionnaire est : 1. Complète et facile, tant pour l'utilisateur final que l'administrateur du SAGU – 15 points 2. Complet et facile, soit pour l'utilisateur final ou l'administrateur du SAGU – 10 points	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	Formulaire d'évaluation de l'exercice Rapport après action Plan d'action de la gestion Plan de communication Plan de l'exercice	3. Partielle, facile tant pour l'utilisateur final que pour l'administrateur du SAGU – 5 points 4. Partielle, facile pour l'utilisateur final ou l'administrateur du SAGU – 0 point	
R23	Le système proposé par le soumissionnaire doit permettre de : 1. Planifier de la formation et de la sensibilisation; 2. Surveiller et suivre l'exécution des activités énumérées ci-dessous à l'aide d'un produit graphique; 3. Rendre compte des progrès des activités énumérées ci-dessous; et 4. Signaler automatiquement les activités non conformes ou en retard. pour chacun des types d'activités suivants : 1. Activités de formation et de sensibilisation des employés pour les situations d'urgence, notamment : i. Formation sur le SAGU, ii. Séances de sensibilisation aux intrus armés, iii. Intervention de cybersécurité iv. Continuité de la TI. 2. Exercices d'urgence dans l'immeuble, notamment : i. Exercices d'incendie,	Pour les activités énumérées de formation et de sensibilisation des employés en cas d'urgence et les exercices d'urgence dans les immeubles, le système proposé par le soumissionnaire : 1. Comprend les quatre fonctionnalités numérotées qui couvrent les six activités énumérées – 10 points 2. Ne comporte que les fonctionnalités 1, 2 et 3 pour couvrir les six activités énumérées – 8 points 3. Ne comporte que les fonctionnalités 1, 2 et 3, mais la fonctionnalité 2 ne peut surveiller que deux à cinq des activités énumérées – 6 points 4. Ne comporte que les fonctionnalités 1, 2 et 3, mais la fonctionnalité 1 peut permettre de planifier la formation et la sensibilisation des employés ou les exercices d'urgence de l'immeuble et la fonctionnalité 2 ne peut surveiller que deux à cinq des activités énumérées – 4 points	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	ii. Exercices de confinement.	5. Ne comporte que la fonctionnalité 2, qui ne peut surveiller que deux à cinq des activités énumérées – 2 points 6. Ne comporte aucune fonctionnalité indiquée pour aucune des activités indiquées – 0 point	

7.2.1.7. Gestion des données

ID	Exigence	Critères de notation	Justification
R24	Le système proposé par le soumissionnaire doit permettre de créer des relations entre les données ou les renseignements d'EDSC (documents et rapports électroniques) contenus dans le SAGU, notamment : 1. Lieux (p. ex., étage, nom de l'immeuble, type de bâtiment, région géographique définie, ville, province, région géographique définie par EDSC) 2. Services essentiels 3. Dépendances de la TI 4. Responsables des plans de gestion des urgences ou de continuité des activités	Chacun des éléments énumérés vaut 8 points, pour un total de 32 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R25	Le système proposé par le soumissionnaire doit permettre aux administrateurs du SAGU de : 1. Modifier et ajouter des étiquettes de champ sur l'interface utilisateur et les modèles, sans l'aide de l'entrepreneur (fournisseur de couches SaaS);	Le système proposé par le soumissionnaire comporte : 1. Les deux fonctionnalités indiquées – 10 points	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	2. Reproduire les nouvelles étiquettes dans tous les documents électroniques applicables.	2. La première fonctionnalité indiquée seulement – 5 points 3. Aucune des fonctionnalités indiquées – 0 point	
R26	Le système proposé par le soumissionnaire devrait permettre de signaler la conservation de : 1. Documents et rapports électroniques; 2. Métadonnées connexes; 3. Registres de vérification connexes.	Le système proposé par le soumissionnaire comporte : 1. La fonctionnalité complète permettant de signaler les documents électroniques, les métadonnées et les registres de vérification à des fins de conservation – 10 points 2. La fonctionnalité permettant de signaler deux des trois types de fichiers (documents électroniques, métadonnées ou registres de vérification) aux fins de conservation – 6 points 3. La Fonctionnalité permettant de signaler l'un des trois types de fichiers (documents électroniques, métadonnées ou registres de vérification) aux fins de conservation – 3 points 4. Aucune fonctionnalité permettant de signaler les documents électroniques, les métadonnées et les registres de vérification à des fins de conservation – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R27	Le système proposé par le soumissionnaire doit fournir une capacité de saisie et de production de rapports liés aux vérifications qui comprend une piste de vérification pour : 1. Les actions de l'utilisateur 2. Les activités administratives (p. ex., création et modification de comptes d'utilisateur) 3. Les autorisations d'accès de l'utilisateur 4. Les changements de configuration apportés au SAGU. 5. Les modifications du contenu d'EDSC (y compris les données et les documents électroniques d'EDSC) 6. La création de documents électroniques (p. ex., contrôle des versions) 7. L'accès, la modification et la suppression non autorisés des données d'EDSC	Chacun des éléments énumérés vaut 3 points, pour un total de 21 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R28	Le système proposé par le soumissionnaire doit permettre aux utilisateurs d'EDSC de visualiser et de suivre les versions historiques (p. ex., le contrôle des versions) des documents électroniques, y compris les dix versions les plus récentes.	Le système proposé par le soumissionnaire : 1. Peut afficher un nombre défini par l'administrateur de versions historiques des documents, au moins les dix précédentes - 10 points 2. Peut afficher un nombre fixe de versions historiques de documents, au moins les dix précédentes - 8 points 3. Peut afficher un nombre fixe ou défini par l'administrateur de versions historiques des documents, au moins les cinq précédentes - 6 points	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
		4. Peut afficher un nombre fixe ou défini par l'administrateur de versions historiques de documents, au moins les trois précédentes - 3 points 5. Ne peut afficher jusqu'à dix versions historiques de documents – 0 point	
R29	Le système proposé par le soumissionnaire devrait permettre aux administrateurs d'EDSC de configurer le nombre d'actions antérieures que les utilisateurs d'EDSC peuvent annuler.	Le système proposé par le soumissionnaire : 1. Offre la fonctionnalité permettant aux administrateurs d'EDSC de configurer le nombre d'actions antérieures que les utilisateurs d'EDSC peuvent annuler – 10 points 2. N'offre pas aux administrateurs d'EDSC la fonctionnalité permettant de configurer le nombre d'actions antérieures que les utilisateurs d'EDSC peuvent annuler – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R30	Le système proposé par le soumissionnaire devrait permettre de sélectionner des données à partir de listes prédéterminées, notamment : 1. Menus déroulants 2. Listes de sélection 3. Recherche	Chacun des éléments énumérés vaut 6 points, pour un total de 18 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R31	Le système proposé par le soumissionnaire devrait permettre de migrer les données existantes. Le Canada fournira les données au soumissionnaire en format CSV.	Le système proposé par le soumissionnaire : 1. Peut migrer toutes les données existantes prévues, lorsque la fonctionnalité est suffisamment importante pour que l'administrateur du SAGU puisse la	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
		réaliser sans l'aide de l'entrepreneur – 20 points 2. Peut migrer toutes les données existantes prévues, mais la fonctionnalité est telle qu'elle ne peut être réalisée qu'avec l'aide de la ressource professionnelle de l'entrepreneur – 10 points 3. Ne peut migrer aucune donnée existante – 0 point	

7.2.1.8. Flux de travail

ID	Exigence	Critères de notation	Justification
R32	Le système proposé par le soumissionnaire devrait identifier automatiquement (p. ex., signaler) l'état des flux de travaux et des tâches à l'aide d'identificateurs uniques : 1. En retard 2. Terminé 3. Incomplet 4. Approuvé 5. Soumis 6. Prévu 7. En révision 8. En cours	Chacun des éléments énumérés vaut 1 point, pour un total de 8 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R33	Le système proposé par le soumissionnaire devrait permettre de consulter et de produire des rapports sur les activités du flux de travail. Ces flux de travail et rapports incluraient les renseignements suivants : 1. fréquence de l'utilisation; 2. % de plans de gestion des urgences (GU) ou de continuité des activités (CA) approuvés; 3. % de plans de GU et/ou de CA en cours (création/examen); 4. % de plans de GU ou de CA manquants; 5. % d'exercices de GU et/ou de CA prévus; 6. % d'exercices de GU et/ou de CA exécutés dans les délais prévus.	Chacun des éléments énumérés vaut 2 points, pour un total de 12 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R34	Le système proposé par le soumissionnaire doit permettre aux utilisateurs du SAGU de recevoir des notifications automatiques des flux de travail, des tâches et des mesures attribués, ce qui comprendrait l'information suivante : 1. Tâches assignées; 2. Tâches réassignées; 3. Tâches achevées; 4. Tâches acceptées; et 5. Tâches refusées.	Chacun des éléments énumérés vaut 2 points, pour un total de 10 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R35	Le système proposé par le soumissionnaire devrait permettre aux utilisateurs du SAGU d'identifier manuellement (c.-à-d. de signaler) les documents électroniques, les rapports et les données d'EDSC pour les : 1. Mises à jour; 2. Révisions;	Chacun des éléments énumérés vaut 3 points, pour un total de 9 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	3. Demandes de renseignements.		

7.2.1.9. Gestion de comptes

ID	Exigence	Critères de notation	Justification
R36	Le système proposé par le soumissionnaire doit permettre aux administrateurs du SAGU ou aux coordonnateurs du SAGU de créer des comptes d'utilisateur ayant les attributs suivants : 1. Nom 2. Titre du poste 3. Fonction de gestion des urgences 4. Région / direction générale 5. Secteur d'activités 6. Direction 7. Division 8. Rôle du SAGU (se référer aux définitions sous Rôles du SAGU, à la page 4) 9. Date d'expiration de l'accès au SAGU 10. Coordonnées : i. Courriel; et ii. Numéros de téléphone. 11. Lieu de travail : i. Ville; ii. Province; iii. Numéro civique et nom de la rue; iv. Étage; et v. Numéro du local ou du bureau.	Chacun des éléments énumérés vaut 1 point, pour un total de 11 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R37	Le système proposé par le soumissionnaire doit permettre aux administrateurs du SAGU d'attribuer les privilèges suivants de compte d'utilisateur, en fonction des rôles : Administrateur du SAGU, coordonnateur du SAGU, contributeur au SAGU, examinateur du SAGU : 1. Accès en lecture 2. Contribuer (p. ex., modifier et signaler les documents électroniques) 3. Créer un document électronique 4. Soumettre un document électronique 5. Approuver un document électronique 6. Accorder ou retirer des privilèges 7. Modifier les propriétés des documents électroniques 8. Attribuer les tâches suivantes aux utilisateurs : i. Remplir un document électronique ii. Mettre à jour un document électronique iii. Réviser un document électronique iv. Approuver un document électronique v. Ajouter des renseignements supplémentaires aux documents électroniques 9. Modifier une tâche 10. Supprimer une tâche 11. Téléverser/télécharger les données/documents électroniques d'EDSC	Chacun des éléments énumérés vaut 2 points, pour un total de 22 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R38	Le système proposé par le soumissionnaire doit permettre aux administrateurs du SAGU de retirer les privilèges des comptes d'utilisateur des utilisateurs du SAGU, sans qu'il soit nécessaire de retirer les privilèges du profil d'un fichier individuel.	Le système proposé par le soumissionnaire : 1. Offre aux administrateurs une fonctionnalité permettant de retirer des comptes d'utilisateur sans avoir à retirer les privilèges dans les fichiers individuels – 10 points 2. Offre à l'entrepreneur une fonctionnalité permettant de retirer les comptes d'utilisateur sans avoir à retirer les privilèges dans les fichiers individuels – 5 points 3. N'offre aucune fonctionnalité permettant de retirer les comptes d'utilisateur sans avoir à retirer les privilèges dans les fichiers individuels – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R39	Le système proposé par le soumissionnaire devrait permettre aux administrateurs du SAGU de restreindre l'accès aux données, aux documents électroniques et aux rapports d'EDSC en fonction de critères prédéfinis (p. ex., groupes – division, direction, direction générale/région, immeuble).	Le système proposé par le soumissionnaire : 1. Peut restreindre l'accès en fonction de tous les critères prédéfinis pour l'organisation et l'immeuble – 20 points 2. Peut restreindre l'accès en fonction soit de l'immeuble ou de critères organisationnels - 10 points 3. Ne peut restreindre l'accès en fonction de critères prédéfinis – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R40	Le système proposé par le soumissionnaire devrait permettre la gestion des comptes d'utilisateur, y compris la surveillance et la production de rapports à cet égard.	Le système proposé par le soumissionnaire : 1. Possède des capacités de gestion des comptes d'utilisateur, ce qui comprend la surveillance et la production de rapports – 20 points 2. Possède des capacités de gestion des comptes d'utilisateur, mais ne comprend pas la surveillance et la production de rapports – 10 points 3. Ne possède aucune capacité de gestion des comptes d'utilisateur – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R41	Le système proposé par le soumissionnaire doit permettre aux administrateurs du SAGU d'interroger les comptes d'utilisateur en filtrant sur ce qui suit : 1. État des flux de travaux (y compris les tâches attribuées) 2. Dates d'ouverture de session 3. Titre du poste 4. Fonction de gestion des urgences 5. Région / direction générale 6. Secteur d'activités 7. Direction 8. Division 9. Rôle du SAGU 10. Date d'expiration de l'accès au SAGU 11. Lieu de travail (c.-à-d. ville, province, numéro civique et nom de rue, étage, numéro de local ou de bureau)	Chacun des éléments énumérés vaut 1 point, pour un total de 11 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
R42	Le système proposé par le soumissionnaire devrait permettre aux utilisateurs du SAGU de récupérer leur mot de passe en libre-service.	Le système proposé par le soumissionnaire : 1. Offre une fonction libre-service de récupération de mot de passe pour les utilisateurs d'EDSC – 10 points 2. Offre une fonctionnalité manuelle de récupération ou de réinitialisation du mot de passe qui doit être effectuée par les administrateurs – 5 points 3. N'offre aucune fonctionnalité de récupération de mot de passe en libre-service pour les utilisateurs d'EDSC – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2.1.10. Interface utilisateur

ID	Exigence	Critères de notation	Justification
R43	Le système proposé par le soumissionnaire doit posséder les capacités suivantes concernant l'interface utilisateur graphique/tableau de bord : 1. Configurabilité selon le type d'utilisateur 2. Visualisation et analyse des points de données du SAGU (p. ex., plans de continuité des activités achevés, flux de travail exécutés)	Le système proposé par le soumissionnaire : 1. Permet de configurer les interfaces utilisateur graphiques/tableaux de bord en fonction du type d'utilisateur et de visualiser et d'analyser les points de données de service du SAGU – 10 points 2. Offre la fonctionnalité de visualisation et d'analyse des points de données de service du SAGU, mais pas de configuration des interfaces utilisateur graphiques/tableaux de bord selon le type d'utilisateur – 5 points 3. Ne comporte aucune fonctionnalité permettant de configurer les interfaces utilisateur graphiques/tableaux de bord ou de visualiser les points de données de service du SAGU – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R44	Le système proposé par le soumissionnaire doit fonctionner[1] sur : 1. Les appareils mobiles personnels – c.-à-d. connectés directement par l'entremise d'un fournisseur de services Internet; et 2. Les appareils mobiles émis par le Canada, connectés par le réseau canadien.	Le système proposé par le soumissionnaire : 1. Peut fonctionner sur des appareils mobiles personnels et des appareils émis par le Canada – 10 points 2. Peut fonctionner sur des appareils mobiles émis par le Canada ou des appareils personnels – 5 points	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	[1], y compris la capacité de traiter des données jusqu'au niveau de confidentialité Protégé B.	3. Ne peut fonctionner sur aucun appareil mobile – 0 point	
R45	Le soumissionnaire doit confirmer son intention de rendre sa solution SaaS conforme à l'instrument de politique du gouvernement du Canada pour l'accès des appareils mobiles au SaaS pouvant respecter les exigences relatives aux données Protégé B du Canada.	1. Le soumissionnaire confirme son intention – 10 points. 2. Le soumissionnaire ne peut confirmer son intention – 0 point.	Le soumissionnaire doit démontrer sa conformité en indiquant son intention.
R46	Le système proposé par le soumissionnaire doit permettre de reconnaître les appareils mobiles et de fournir automatiquement le contenu et les fonctionnalités du SAGU adaptés à l'affichage de l'appareil.	Le système proposé par le soumissionnaire : 1. Est capable de reconnaître automatiquement un appareil mobile et de fournir du contenu qui convient le mieux à son affichage – 10 points 2. Est capable de reconnaître automatiquement un appareil mobile, mais ne peut pas fournir le contenu qui convient le mieux à son affichage – 5 points 3. N'est pas capable de reconnaître automatiquement un appareil mobile ni de fournir le contenu qui convient le mieux à son affichage – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R47	Le système proposé par le soumissionnaire devrait permettre aux utilisateurs du SAGU de télécharger en toute sécurité[1] des documents et rapports électroniques pour une utilisation hors ligne sur des appareils mobiles et des ordinateurs de bureau. [1] Le téléchargement sécurisé est défini à la	Le système proposé par le soumissionnaire : 1. Peut télécharger des documents pour utilisation hors ligne – 10 points	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
	section 7.1.1, Tableau 1 – Exigences relatives à la conformité en matière de sécurité.	2. Ne permet pas de télécharger des documents pour utilisation hors ligne – 0 point	
R48	Le système proposé par le soumissionnaire devrait disposer d'outils d'aide et de formation en ligne pour les utilisateurs du SAGU, avec leur disponibilité comme suit : 1. Conseils sur le positionnement du curseur intégrés au système proposé 2. Fichiers d'aide intégrés ou liés au site Web du soumissionnaire 3. Guides/manuels intégrés ou liés au site Web du soumissionnaire 4. Modules de formation liés au site Web du soumissionnaire	Chacun des éléments énumérés vaut 3 points, pour un total de 12 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

7.2.1.11 Accessibilité

ID	Exigence	Critères de notation	Justification
R49	Le soumissionnaire doit fournir des services de soutien technique aux administrateurs du SAGU dans la langue canadienne de leur choix par téléphone, courriel, messagerie mobile ou outils Web, selon le cas.	Le soumissionnaire peut fournir des services de soutien technique dans : 1. Les deux langues officielles du Canada – 10 points 2. L'une ou l'autre des langues officielles du Canada – 5 points. 3. Aucune langue officielle du Canada – 0 point.	

7.2.2. Exigences non fonctionnelles – Cotées

ID	Exigence	Critères de notation	Justification
R50	Le système proposé par le soumissionnaire doit permettre d'importer/exporter des données/de l'information dans les formats de fichier suivants[1] : 1. .pdf 2. .doc/.docx 3. .csv 4. .xml 5. .xls 6. .ppt 7. .msg 8. Formats de fichier image : .jpeg ou .tiff ou .bmp ou .png 9. Formats de fichiers vidéo : .mpeg ou .avi ou mp4 10. Formats de fichiers audio : .mp3 ou .wav ou .aiff [1] tout nombre de formats pris en charge dans un élément de liste est compté comme un seul.	Chacun des éléments énumérés vaut 2 points, pour un total de 20 points.	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R51	Le système proposé par le soumissionnaire devrait avoir un temps de disponibilité d'au moins 99 %.	Le service du SAGU offre un temps de disponibilité de : 1. 99,999 % - 10 points 1. > 99,99 % - 8 points 2. > 99,9 % - 6 points 3. = 99 % - 3 points 4. < 99 % - 0 point	Le soumissionnaire doit démontrer le niveau de conformité dans son entente sur les niveaux de service publiée.
R52	Le système proposé par le soumissionnaire doit assurer un objectif de point de reprise d'au plus 24 heures en cas de sinistre.	Le système proposé par le soumissionnaire :	Le soumissionnaire doit démontrer le niveau de conformité dans son entente sur les niveaux de service publiée.

ID	Exigence	Critères de notation	Justification
		1. Peut atteindre un objectif de point de reprise du service du SAGU de moins de 4 heures – 10 points 2. Peut atteindre un objectif de point de reprise du service du SAGU de 4 à 8 heures – 8 points 3. Peut atteindre un objectif de point de reprise du service du SAGU de 8 à 24 heures – 6 points 4. Impossible d'atteindre un objectif de point de reprise du service du SAGU de 24 heures ou moins – 0 point	
R53	Le système proposé par le soumissionnaire doit fonctionner avec les navigateurs de bureau suivants, les versions indiquées ou plus récentes : 1. Internet Explorer v11 2. Microsoft Edge Chromium 93.0.961.47 3. Safari v10 4. Chrome 93.0.4577.82 5. Firefox Quantum 92	Le système proposé par le soumissionnaire : 1. Fonctionne dans tous les navigateurs indiqués – 10 points. 2. Fonctionne dans au moins trois des navigateurs énumérés – 6 points 3. Fonctionne seulement dans Internet Explorer v10 - 3 points 4. Ne fonctionne avec aucun des navigateurs indiqués – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R54	Le système proposé par le soumissionnaire devrait fonctionner dans les navigateurs mobiles compatibles avec les systèmes d'exploitation mobiles suivants : 1. Android 2. Système d'exploitation BlackBerry 3. iOS 4. Windows Mobile	Le système proposé par le soumissionnaire : 1. Fonctionne avec des navigateurs mobiles compatibles avec les quatre systèmes d'exploitation mobiles indiqués – 10 points 2. Fonctionne avec des navigateurs mobiles compatibles avec au moins	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

ID	Exigence	Critères de notation	Justification
		trois des systèmes d'exploitation mobiles indiqués – 5 points 3. Ne fonctionne avec aucun des navigateurs mobiles compatibles avec les systèmes d'exploitation mobiles indiqués – 0 point	
R55	Le système proposé par le soumissionnaire devrait prendre en charge les fichiers joints d'une taille pouvant atteindre 5 mégaoctets sans avertissement et les fichiers joints de taille supérieure à 5 mégaoctets devraient déclencher un avertissement pour l'utilisateur. Les administrateurs devraient être en mesure de définir les seuils des avertissements.	Le système proposé par le soumissionnaire : 1. Prend en charge les pièces jointes et déclenche des avertissements de taille de fichier pour les pièces jointes supérieures à 5 mégaoctets, avec la flexibilité que le seuil soit défini par un administrateur du SAGU – 10 points 2. Prend en charge les pièces jointes et déclenche des avertissements de taille de fichier pour les pièces jointes supérieures à 5 mégaoctets, mais les seuils ne sont que ceux prédéfinis par l'entrepreneur – 8 points 3. Prend en charge les pièces jointes de plus de 5 mégaoctets, mais ne peut émettre d'avertissements pour ceux-ci – 6 points 4. Ne prend pas en charge les fichiers joints et n'émet pas d'avertissements relatifs à la taille des fichiers – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R56	Le système proposé par le soumissionnaire devrait permettre à l'administrateur du SAGU de	Le système proposé par le soumissionnaire :	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des

ID	Exigence	Critères de notation	Justification
	configurer une période d'inactivité après laquelle une session d'utilisateur prend fin.	1. Offre cette fonctionnalité – 10 points 2. N'offre pas cette fonctionnalité – 0 point.	saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.
R57	Le soumissionnaire doit offrir au Canada, sans frais supplémentaires, les environnements d'essai suivants : 1. Environnement d'essai fonctionnel 2. Environnement de mise à l'essai de performance du système	Le soumissionnaire fournira : 1. Les deux environnements d'essai – 10 points 2. Un seul environnement d'essai – 5 points 3. Aucun environnement d'essai – 0 point	Le soumissionnaire doit démontrer sa conformité en documentant sa capacité de répondre aux exigences, en utilisant des saisies d'écran ou des documents techniques ou d'utilisateur final pour compléter ses réponses.

Un soumissionnaire sera jugé qualifié pour réussir l'évaluation de la soumission financière s'il obtient au moins 75 % (ou 682) du total maximal des exigences cotées de 910 points.

8. ÉNONCÉ DES TRAVAUX

8.1 Documents de référence

Les documents de référence suivants sont pertinents pour le présent énoncé des travaux :

8.1.1. Le système du soumissionnaire ne doit pas empêcher le Canada (EDSC dans le présent contrat) de s'acquitter de ses obligations décrites dans les instruments de politique suivants du Canada.

1. Gestion des urgences (GU) :
   - i. Loi sur la gestion des urgences (2007)
   - ii. Politique fédérale en matière de gestion des urgences (2009)
   - iii. Politique sur la sécurité du gouvernement (2019)

2. Gestion de la continuité des activités (GCA)
   i. Directive sur la gestion de la sécurité - Annexe D : Procédures obligatoires pour le contrôle de la gestion de la continuité des activités (2019)
3. Équipes d'urgences et d'évacuation de immeubles (EEUI) :
   i. Code canadien du travail (1985)
   ii. Loi sur les immeubles fédéraux et les biens réels fédéraux (1991)
   iii. Règlement canadien sur la santé et la sécurité au travail (2012)
   iv. Norme pour le plan d'évacuation d'urgence et l'organisation des secours en cas d'incendie — Chapitre 3.1 du Conseil du Trésor (1994)
4. Protection contre les incendies :
   i. Norme sur la protection contre les incendies du Conseil du Trésor (2019)
   ii. Code national de prévention des incendies (2010)
   iii. Code national du bâtiment — Canada (2010)
   iv. Politique du Conseil du Trésor sur la gestion des biens immobiliers (2019)

Le système proposé par le soumissionnaire ne devrait pas empêcher le Canada de se conformer aux instruments de politique suivants :

5. Loi sur l'accès à l'information
6. Loi sur les langues officielles
7. Loi sur la protection des renseignements personnels
8. Directive sur la gestion des communications
9. Politique sur l'accès à l'information
10. Politique sur la gestion de l'information
11. Règles pour l'accessibilité des contenus Web (WCAG) 2.0 (en anglais seulement)
12. Lignes directrices concernant la conservation des documents administratifs communs de l'administration fédérale
13. Norme sur la facilité d'emploi des sites Web
14. Boîte à outils de l'expérience Web – Ligne directrice

15. Normes sur la protection de la vie privée et le Web analytique
16. Loi sur le ministère de l'Emploi et du Développement social
17. Loi sur la Bibliothèque et les Archives du Canada
18. Norme sur l'assurance de l'identité et des justificatifs
19. Norme sur le filtrage de sécurité
20. Algorithmes cryptographiques pour les renseignements non classifiés, Protégé A et Protégé B
21. Norme sur les métadonnées
22. Directive sur la tenue de documents

8.2 Portée des travaux

Au moment de l'attribution du contrat et avant que le Canada accepte le système mis en œuvre, l'entrepreneur doit exécuter les travaux suivants : L'entrepreneur devra fournir les travaux et services suivants, conformément aux plans acceptés par le Canada et énumérés dans le tableau 2 ci-dessous.

Les travaux à effectuer et les services à fournir entre la signature du contrat et la mise en production sont les suivants :

8.2.1 Une fois l'abonnement payé pour les 20 utilisateurs principaux initiaux, créer un accès au système (comptes d'utilisateur) pour ceux-ci

8.2.2 Former les 20 utilisateurs principaux

8.2.3 Configurer le SAGU

8.2.4 Assurer la migration des actifs informationnels du Canada vers le SAGU

8.2.5 Une fois l'abonnement payé pour les 2 980 autres utilisateurs, créer un accès au système (comptes d'utilisateur) pour ceux-ci

8.2.6 Si l'entrepreneur l'offre au Canada, établir les environnements d'essai fonctionnel et de rendement du SAGU

8.2.7 Si des environnements d'essai sont configurés, mettre à l'essai la fonctionnalité et le rendement du SAGU, au besoin et sur demande au moyen du processus d'autorisation de tâches

8.2.8 Aider le Canada à former les 2 980 autres utilisateurs, sur demande, dans le cadre du processus d'autorisation des tâches

8.2.9 Aider au déploiement du service du SAGU, sur demande, dans le cadre du processus d'autorisation des tâches.

8.2.10 Fournir des services de dépannage, au besoin

8.2.11 Fournir des services de soutien technique, au besoin

Les travaux à effectuer et les services à fournir après la production et pendant la durée du contrat sont les suivants :

8.2.12 Fournir des services de dépannage (bilingues), au besoin
8.2.13 Fournir des services de soutien technique (bilingues), au besoin

8.3 Produits livrables

Dans chacun des plans énumérés ci-dessous, l'entrepreneur inclura un calendrier interne des activités pertinentes en ce qui a trait à la date d'attribution du contrat.

Au moment de l'attribution du contrat, le Canada présidera une petite série de réunions de lancement de projet au cours desquelles il consultera l'entrepreneur et où les échéanciers des plans soumis pourront être rajustés afin d'être intégrés à un calendrier de projet final.

On s'attend à ce que l'entrepreneur fournisse des ressources qualifiées pour fournir un service de qualité dans les délais mutuellement convenus précisés dans les plans acceptés.

Tableau 2 – Calendrier des produits livrables

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
8.3.1	Plan de formation sur le SAGU	Le plan doit veiller à ce que la formation soit suffisamment complète pour que les stagiaires du Canada puissent : i. Utiliser toutes les caractéristiques fonctionnelles et administratives; ii. Configurer et adapter le SAGU; iii. Migrer les actifs informationnels existants; iv. Fournir une assistance technique aux autres utilisateurs du Canada. Le soumissionnaire proposera les meilleures façons d'offrir la formation relativement à l'emplacement au Canada. Au moment de l'attribution du contrat, l'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre avec la soumission. Finaliser après les ateliers de lancement.
8.3.2	Plan de mise en œuvre du SAGU	Le plan doit décrire la façon dont l'entrepreneur envisage toutes les activités pertinentes à la mise en œuvre, sans se limiter à ce qui suit : i. Création d'un accès au système pour les utilisateurs; ii. Configuration du SaaS générique de l'entrepreneur dans le SAGU en tant que service du Canada (c.-à-d. service du GC); iii. Migration des actifs informationnels du Canada vers le SAGU; iv. Transfert et synchronisation avec le SAGU des données de la plateforme de gestion de l'identité du Canada (Microsoft Active Directory) nécessaires à l'authentification de l'accès au système;	Document	Soumettre avec la soumission.

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
		v. Activation du SAGU pour recevoir les mises à jour hebdomadaires d'EDSC de certaines données sur le personnel sous forme de fichier CSV chiffré. Au moment de l'attribution du contrat, l'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.		Finaliser après les ateliers de lancement.
8.3.3	Plan de réalisation des tests pour le SAGU	Le plan doit décrire la façon dont l'entrepreneur envisage au moins les activités suivantes : i. Définition et configuration de tous les environnements d'essai offerts; ii. Définition des types d'essai offerts (p. ex., fonctionnel, rendement) et identification des rôles (entrepreneur et Canada) pour chaque type d'essai. iii. Définition des cas d'essai et moment estimé de leur exécution. iv. Au moment de l'attribution du contrat, l'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre avec la soumission. Finaliser après les ateliers de lancement.
8.3.4	Plan de déploiement du SAGU	Le plan doit décrire la façon dont l'entrepreneur envisage la mise en œuvre auprès de 3 000 utilisateurs formés. Au moment de l'attribution du contrat, l'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre avec la soumission. Finaliser après les ateliers de lancement.
8.3.5	Réunions de lancement du projet	L'entrepreneur participera à la série de réunions de type atelier présidées par le Canada, au cours desquelles il discutera et conviendra de plus amples détails sur les produits livrables susmentionnés et leur calendrier d'exécution. L'entente entraînera probablement une certaine modification des échéanciers fournis par l'entrepreneur dans ses plans soumis afin de les harmoniser avec le calendrier global prévu du projet.	Réunions	Commencer dans les cinq jours ouvrables suivant la signature du contrat.
8.3.6	Accès au système pour	Après 20 abonnements payés, il faut créer un accès au système (comptes d'utilisateur) pour les 20 premiers utilisateurs.	Comptes d'utilisateurs	Dans les trois jours ouvrables suivant la

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
	20 utilisateurs principaux			signature du contrat.
8.3.7	Plan de continuité des activités du SAGU et plan de reprise après sinistre	Les plans doivent comprendre au moins les renseignements suivants : i. Le temps de reprise après une interruption; ii. Le temps nécessaire pour passer à un site de sauvegarde; iii. Le niveau de service et la fonctionnalité fournis par le site de sauvegarde et période pendant laquelle le répondant récupérera les données primaires et le service principal; iv. Rapport sur la méthode et la fréquence à laquelle l'entrepreneur met à l'essai ou exerce ces plans L'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre dans les dix jours ouvrables suivant la date d'attribution du contrat.
8.3.8	Guide de l'administrateur du SAGU	Le guide doit décrire tout ce qu'un administrateur du SAGU doit accomplir dans ce rôle. L'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre dans les dix jours ouvrables suivant l'attribution du contrat.
8.3.9	Guide de l'utilisateur du SAGU	Le guide doit décrire tout ce qui est nécessaire pour qu'un utilisateur du SAGU puisse utiliser ce service conformément à ce qui est défini dans l'énoncé des besoins. L'entrepreneur et le Canada pourraient devoir faire des mises à jour avant que le Canada accepte le plan final.	Document	Soumettre dix jours ouvrables après l'attribution du contrat.
8.3.10	Formation de base	Guidé par le plan de formation du SAGU, l'entrepreneur doit former 20 utilisateurs principaux afin qu'ils deviennent des administrateurs du SAGU, qui pourront alors : - aider l'entrepreneur à configurer le SAGU et à migrer ses actifs informationnels; - effectuer des essais fonctionnels et de rendement (si des environnements d'essai sont offerts au Canada); et - former les 2 980 autres utilisateurs.	Services professionnels	Le début et la durée seront conformes au plan de formation du SAGU accepté par le Canada; le Canada prévoit que la durée sera d'au plus cinq jours ouvrables.

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
8.3.11	Configuration du SAGU	Guidé par le plan de mise en œuvre du SAGU, l'entrepreneur doit configurer son SaaS dans le SAGU pour devenir un service du Canada (c.-à-d. un service du GC). La configuration sera effectuée de manière à satisfaire aux exigences énoncées dans l'énoncé des besoins pour lesquelles le soumissionnaire a affirmé qu'il se conformait. La configuration doit être effectuée dans les délais prévus dans le calendrier principal du projet du Canada, harmonisée avec les ressources désignées de l'entrepreneur, qualifiées pour configurer le SaaS commercial dans le SAGU du Canada, exécutera cette activité dans le cadre de ses services de mise en œuvre et de configuration. Il n'y aura pas de rappel pour cette activité et l'entrepreneur peut choisir de préciser les frais séparément ou dans le cadre des frais d'abonnement. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de mise en œuvre du SAGU afin d'éclairer le plan final accepté par le Canada.	Services professionnels	Le début et la durée seront conformes au plan de mise en œuvre du SAGU accepté par le Canada. Le Canada estime que la durée ne peut pas dépasser 15 jours ouvrables.
8.3.12	Migration des actifs informationnels du Canada	Guidé par le plan de mise en œuvre du SAGU, l'entrepreneur doit migrer les ressources d'information du Canada (données et information existantes, données de la plateforme de gestion de l'identité du Canada (fondée sur Microsoft Active Directory) nécessaires à l'authentification des utilisateurs). La migration doit être effectuée dans les délais prévus dans le calendrier principal du projet du Canada, conformément au plan de mise en œuvre du SAGU accepté par le Canada. Les ressources désignées de l'entrepreneur, qualifiées pour migrer les actifs informationnels du Canada au SAGU du Canada, exécuteront cette activité dans le cadre de leurs services de mise en œuvre ou de configuration. Il n'y aura pas de rappel pour cette activité et l'entrepreneur peut choisir de préciser les frais séparément ou dans le cadre des frais d'abonnement. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de mise en œuvre du SAGU afin d'éclairer le plan final accepté par le Canada.	Services professionnels	Le début et la durée seront conformes au plan de mise en œuvre du SAGU accepté par le Canada. Le Canada estime qu'il ne durera pas plus de 20 jours ouvrables.
8.3.13	Mise à l'essai du SAGU – Fonctionnel et rendement	Guidé par le plan d'essai du SAGU, l'entrepreneur doit : i. (s'ils sont offerts au Canada dans leur soumission) Établir des environnements d'essai pour les essais fonctionnels et de rendement;	Services professionnels	Le début et la durée seront conformes au plan d'essai du SAGU

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
		ii. Être disponible au Canada et aider au besoin à effectuer les essais fonctionnels et de rendement de l'application logicielle (service). Les ressources désignées par l'entrepreneur et qualifiées pour soutenir le Canada en ce qui concerne les essais seront sollicitées uniquement si le Canada fait face à des problèmes qu'il ne peut résoudre lui-même. Le temps consacré par la ressource de l'entrepreneur sera surveillé par l'État et une fois les essais terminés, il sera approuvé par le Canada pour être facturé à l'heure. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan d'essai du SAGU afin d'éclairer le plan final accepté par le Canada.		accepté par le Canada. Le Canada estime qu'il ne durera pas plus de 35 jours ouvrables.
8.3.14	Accès au système pour les 2 980 autres utilisateurs	Sur paiement pour les 2 980 abonnements, l'entrepreneur doit créer un accès au système (comptes d'utilisateur) pour les 2 980 autres utilisateurs. Cette activité doit se dérouler dans les délais prévus dans le calendrier principal du projet du Canada, conformément au plan de mise en œuvre du SAGU accepté par le Canada.	Services professionnels	Le début et la durée seront conformes au plan de mise en œuvre du SAGU, accepté par le Canada. Le Canada estime qu'il ne durera pas plus de dix jours ouvrables.
8.3.15	Formation de masse des utilisateurs	Guidé par le plan de formation du SAGU, l'entrepreneur doit appuyer le Canada, au besoin, dans la prestation de la formation aux autres utilisateurs. Les formateurs désignés du Canada, eux-mêmes formés à titre de 20 utilisateurs principaux, offriront la formation aux autres utilisateurs. Les ressources désignées de l'entrepreneur, qualifiées pour appuyer le Canada en matière de formation, ne seront sollicitées que si le Canada fait face à des problèmes qu'il ne peut résoudre lui-même. Le temps consacré par la ressource de l'entrepreneur sera surveillé par l'État et une fois la formation terminée, il sera approuvé par le Canada pour être facturé à l'heure. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de formation du SAGU afin d'éclairer le plan final accepté par le Canada.	Services professionnels	Le début et la durée seront conformes au plan de formation du SAGU accepté par le Canada. Le Canada estime qu'il pourrait ne pas durer plus de 60 jours ouvrables.

N°	Titre du produit livrable	Description du produit livrable	Type de produit livrable	Date d'échéance
8.3.16	Déploiement du SAGU	Guidé par le plan de déploiement du SAGU, l'entrepreneur doit déployer le service du SAGU auprès de tous les autres utilisateurs définis (soit 2 980 utilisateurs). Cette activité doit se dérouler dans les délais prévus dans le calendrier principal du projet du Canada, conformément au plan de déploiement du SAGU accepté par le Canada. Les ressources désignées par l'entrepreneur, qualifiées pour soutenir le Canada dans le cadre du déploiement, ne seront sollicitées que si le Canada fait face à des problèmes qu'il ne peut résoudre lui-même. Le temps consacré par la ressource de l'entrepreneur sera surveillé par l'État et une fois la formation terminée, il sera approuvé par le Canada pour être facturé à l'heure. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de déploiement du SAGU afin d'éclairer le plan final accepté par le Canada.	Services professionnels	Le début et la durée seront conformes au plan de déploiement du SAGU accepté par le Canada. Le Canada suppose qu'un utilisateur ne peut être déployé avant d'avoir reçu une formation. Le Canada estime que le déploiement complet de 2 980 utilisateurs pourrait ne pas durer plus de 30 jours ouvrables.
8.3.17	Entrée en service	L'entrepreneur doit aider le Canada, au besoin, à mettre le SAGU en service. Les ressources désignées par l'entrepreneur, qualifiées pour soutenir le Canada en ce qui concerne le lancement de la production, seront sollicitées uniquement si le Canada fait face à des problèmes qu'il ne peut résoudre lui-même. Le temps consacré par la ressource de l'entrepreneur sera surveillé par l'État et une fois la formation terminée, il sera approuvé par le Canada pour être facturé à l'heure. L'entrepreneur pourrait vouloir définir son processus de choix dans le plan de déploiement du SAGU afin d'éclairer le plan final accepté par le Canada.	Services professionnels	Débute à l'achèvement du déploiement (mais au plus tard une semaine après celui-ci) et après l'obtention de l'autorisation d'exploitation; dure un jour ouvrable.

8.4 Appui fourni par EDSC

Dans ses locaux au Canada, le Canada fournira l'équipement informatique et la connectivité réseau adéquate au SAGU ainsi que la bande passante requise pour la formation sur place de ses utilisateurs désignés comme administrateurs du SAGU.

Le Canada déterminera, en consultation avec l'entrepreneur, quelles données et/ou informations et quels documents de référence pertinents seront nécessaires pour mener à bien la formation de base et fournira les éléments convenus.

8.5 Contraintes

L'entrepreneur doit tenir compte des contraintes suivantes du projet et s'y conformer :

8.5.1 L'entrepreneur doit fournir les documents énumérés à la section 3.1 et tout autre document jugé conjointement par l'entrepreneur et le Canada comme nécessaire à l'exécution réussie des tâches énumérées, en anglais et en français, en version électronique, à l'adresse de l'autorité contractante du SAGU précisée dans le document principal de la DP.

8.5.2 L'entrepreneur n'aura aucun accès physique à aucun des sites du Canada faisant partie du réseau du Canada. L'entrepreneur peut avoir accès, physiquement ou à distance, à l'instance du SAGU du Canada dans son nuage public, mais seulement pour le personnel ayant reçu le contrôle sécuritaire adéquat de personnel du Canada. Pour plus de détails, veuillez consulter la section Exigences relatives à la sécurité de l'énoncé des besoins et le document principal de la DP.

Annexe A – Glossaire

Terme	Définition
NVSA	Norme de vérification de la sécurité des applications
GCA	Gestion de la continuité des activités
PCA	Plan de continuité des activités
PEUI	Plans d'évacuation d'urgence des immeubles
ARA	Analyse des répercussions sur les activités
CCC	Centre canadien pour la cybersécurité (anciennement appelé CST ou CSTC)
MCN	Matrice des contrôles du nuage
CIS	Centre for Internet Security
BDGC	Base de données de la gestion de la configuration
DGC	Équipe de gestion de crises
RCR	Réanimation cardio-respiratoire
CSA	Cloud Security Alliance
CST	Centre de la sécurité des télécommunications (anciennement appelé CCCS)
CSTC	Centre de la sécurité des télécommunications Canada
FSI	Fournisseur de services infonuagiques – fournisseur d'un ou de plusieurs services infonuagiques (Iaas, PaaS, SaaS)
CSV	Fichiers de valeurs séparées par des virgules
GU	Gestion des urgences
SAGU	Système d'application pour la gestion des urgences
EDSC	Emploi et Développement social Canada, un ministère du gouvernement du Canada
PFIU	Plan fédéral d'intervention d'urgence
NFTI	Normes fédérales de traitement de l'information
CANADA	Gouvernement du Canada, pour la présente demande de soumissions, désigne également EDSC
IaaS	Infrastructure comme service
ISO	Organisation internationale de normalisation
TI	Technologie de l'information
GCSTI	Gestion de la continuité des services de technologie de l'information
TAMA	Temps d'arrêt maximal admissible
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project

Terme	Définition
PaaS	Plateforme comme service
PBMM	Protégé B, intégrité moyenne, disponibilité moyenne
ICR	Indicateurs clés de rendement
OPR	Objectif de point de reprise
ODR	Objectif de délai de rétablissement
SaaS	Logiciels en tant que service
SAFECode	Forum sur l'assurance logicielle pour l'excellence du Code
SAML	Langage de balisage des assertions de sécurité (Security Assertion Markup Language)
ICA	Intégration des chaînes d'approvisionnement
GRCA	Gestion des risques liés à la chaîne d'approvisionnement
ENS	Entente sur les niveaux de service
PON	Procédure opérationnelle normalisée
TLS	Protocole TLS (Transport Layer Security)
RPV	Réseau privé virtuel

Annexe B – Glossaire

Terme	Définition
Actifs	Les actifs comprennent, sans s'y limiter, l'information de toute forme et les médias, les réseaux, les systèmes, le matériel, les biens réels, les ressources financières, les fiducies d'employés, la confiance du public et la réputation internationale. (Guide pour la planification de la gestion des urgences 2010-2011 de Sécurité publique Canada)
Sensibilisation	Favoriser une compréhension des problèmes et les limites de base de la GCA. Cela permettra au personnel de reconnaître les menaces et de réagir en conséquence. La distribution d'affiches et de dépliants destinés à l'ensemble de l'entreprise ou la tenue de séances d'information précises sur la continuité des activités à l'intention de la haute direction de l'entreprise sont des exemples de cette sensibilisation. La sensibilisation est moins formelle que la formation et vise généralement l'ensemble du personnel.
Direction générale	Une subdivision de premier niveau d'EDSC.
Gestion de la continuité des activités (GCA)	Processus de gestion global qui permet de cerner les menaces potentielles pour une organisation et les répercussions que ces menaces pourraient causer sur les activités opérationnelles, et qui fournit un cadre pour renforcer la résilience organisationnelle et la capacité d'intervention efficace qui protège les intérêts de ses principaux intervenants, la réputation, la marque et les activités de création de valeur.
Plan de continuité des activités (PCA)	Un ensemble documenté de procédures et de renseignements qui est élaboré, compilé et tenu à jour en vue d'une utilisation en cas d'incident pour permettre à une organisation de continuer d'offrir ses produits et services essentiels à un niveau acceptable prédéfini.
Analyse des répercussions sur les activités (ARA)	Une méthode de détermination des conséquences d'un défaut d'exécution d'une fonction ou d'une exigence.
Liste de vérification	1. Outil pour rappeler ou valider que les tâches ont été accomplies et que des ressources sont disponibles pour rendre compte de l'état du rétablissement. 2. Liste des éléments (noms ou tâches, etc.) à vérifier ou à consulter.
Services infonuagiques	Services habituellement inclus dans les modèles de services infonuagiques comme Saas, Paas ou Iaas.
Risques liés à la conformité	Les risques liés à la conformité concernent la conformité juridique et réglementaire.
Base de données de la gestion de la configuration	Base de données utilisée par une organisation pour stocker des renseignements sur le matériel et les logiciels (communément appelés éléments de configuration). Cette base de données sert d'entrepôt de données pour l'organisation et conserve également des renseignements sur les relations entre ses actifs.
Plan de rechange	Plan utilisé par une organisation ou une unité opérationnelle pour réagir à une panne de système particulière ou à une interruption des activités.

Terme	Définition
Gestion de crise	Coordination globale de l'intervention d'une organisation en cas de crise, de manière efficace et en temps opportun, dans le but d'éviter ou de minimiser les dommages à la rentabilité, à la réputation et à la capacité d'exploitation de l'organisation.
L'équipe de gestion de crise (EGC)	Groupe de personnes chargées d'élaborer et de mettre en œuvre un plan complet d'intervention en cas d'incident perturbateur. L'équipe se compose d'un groupe central de décideurs formés en gestion des incidents et prêts à réagir à toute situation.
Direction	Subdivision de premier niveau d'une direction générale.
Planification de la reprise après sinistre	Activités associées à la disponibilité continue et à la planification de la restauration de l'infrastructure de TI.
Division	Subdivision de premier niveau d'une direction.
Documents électroniques	Tout document stocké par le SAGU. Comprend les plans, les rapports, les listes de vérification, les questionnaires, les listes, les calendriers et les modèles de gestion des urgences.
Administrateur du SAGU	Rôle du SAGU, un rôle ayant les privilèges les plus élevés pour l'utilisation du système, y compris la gestion des comptes d'utilisateur.
Guide de l'administrateur du SAGU	Guide adapté au type d'utilisateur de l'administrateur du SAGU.
Contributeur au SAGU	Rôle du SAGU, un rôle comportant des privilèges limités, habituellement dans un domaine opérationnel particulier.
Coordonnateur du SAGU	Rôle du SAGU, avec les privilèges les plus élevés, mais pour un domaine opérationnel particulier.
Calendrier du projet du SAGU	Calendrier de projet élaboré par le CANADA, en consultation avec le fournisseur.
Guide de l'utilisateur du SAGU	Guide adapté aux autres types d'utilisateurs du SAGU, comme le coordonnateur du SAGU, le contributeur du SAGU, le visualiseur du SAGU.
Visualiseur du SAGU	Rôle du SAGU, un rôle comportant uniquement des droits d'accès en lecture seule.
Gestion des urgences (GU)	1. Processus continu de prévention, d'atténuation, de préparation, d'intervention, de continuité et de reprise après un incident qui menace la vie, les biens, les opérations ou l'environnement. (NFPA 1600) 2. Programme qui met en œuvre la mission, la vision, les buts stratégiques, les objectifs et le cadre de gestion du programme et de l'organisation.
Activités de gestion des urgences (GU)	Cela inclut : 1. Exercices d'urgence a) Continuité des activités b) Gestion des urgences c) Continuité de la TI 2. Cycles de création et d'examen des documents électroniques 3. Formation de l'équipe d'évacuation d'urgence de l'immeuble 4. Activités de sensibilisation à la gestion des urgences

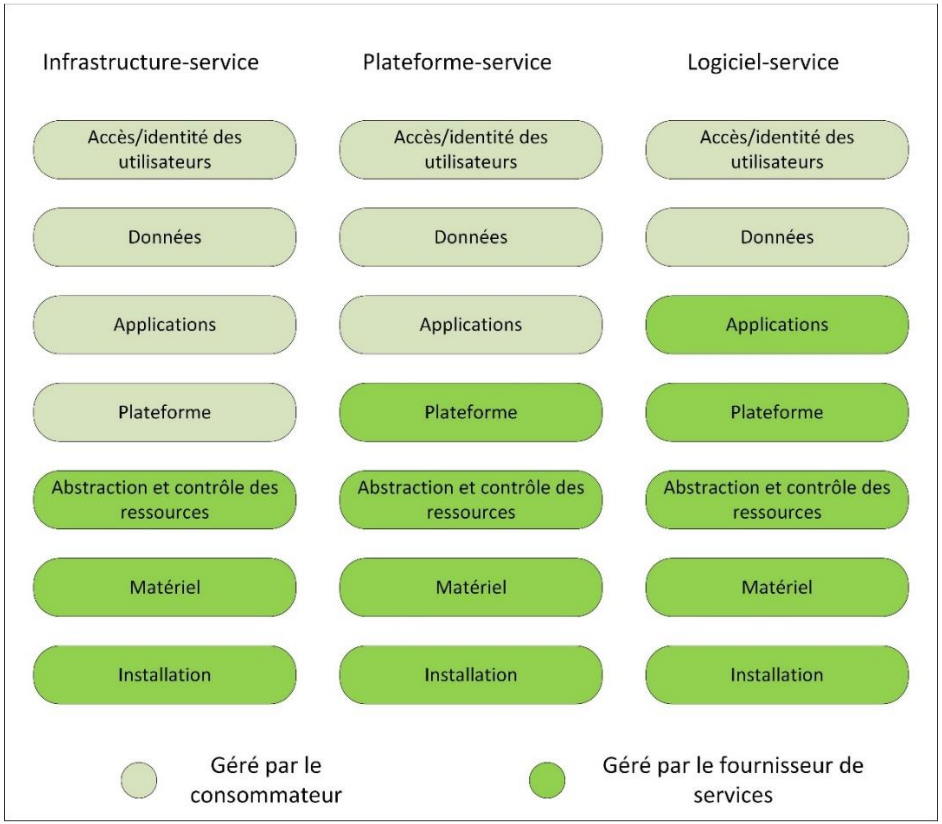
Terme	Définition
Plans de gestion des urgences	Cela inclut : 1. Plan de continuité des activités (PCA) 2. Analyse des répercussions sur les activités (ARA) 3. Continuité de la TI 4. Plan d'évacuation d'urgence de l'immeuble (PEUI) 5. Plans d'urgence 6. Plans d'action
Emploi et Développement social Canada (EDSC)	Un ministère du gouvernement du Canada qui sollicite un système dans le cadre de cet approvisionnement.
Exercice	Activité au cours de laquelle le ou les plans de l'entité sont mis en œuvre en tout ou en partie pour s'assurer qu'ils contiennent l'information appropriée et produisent le résultat souhaité lorsqu'ils sont mis en œuvre.
Exercices à grande échelle	Un exercice à grande échelle est un exercice multi-organismes, multijuridictionnel et multidisciplinaire faisant appel à des fonctions (p. ex., bureau conjoint sur le terrain, centres des opérations d'urgence) et à des interventions « sur le terrain » (p. ex., des employés de la continuité qui déménagent dans leurs autres sites pour exécuter des fonctions essentielles axées sur des scénarios).
Incidence sur le bien-être économique des Canadiens/du public	Comprend les services économiques, monétaires et financiers essentiels et fondamentaux requis pour maintenir la sécurité du revenu, la stabilité économique, les services bancaires essentiels et les programmes de prestations parrainés par le gouvernement requis pour maintenir le mieux-être des Canadiens et éviter un préjudice élevé.
Incidence sur le fonctionnement du gouvernement ou de l'organisation	Comprend les services gouvernementaux essentiels, les accords constitutionnels, les programmes, les politiques, les règlements, la législation et l'affectation des ressources humaines et financières requises pour maintenir l'efficacité du gouvernement et éviter un préjudice élevé.
Incidence sur la santé des Canadiens/du public	Renvoie aux services « de soins et d'intervention d'urgence » requis pour assurer la subsistance et pour éviter les blessures. Cela comprend les services d'urgence nécessaires pour sauver des vies et pour rétablir le « fonctionnement » normal des personnes à la suite d'un traumatisme ou d'un accident grave.
Incidence sur la conformité juridique et réglementaire du Ministère/organisme	Comprend la législation, la politique directrice, les litiges et les obligations (PE, ententes, traités, contrats, clients internes/externes).
Incidence sur la confiance et la réputation du public dans le Ministère ou l'organisation	Renvoie à l'évaluation subjective que fait la population de la crédibilité du gouvernement et de sa capacité d'offrir des services.
Incidence sur la sûreté des Canadiens/du public	Comprend les services essentiels (comme les services d'incendie, la police, les ambulances) et les services de sécurité généraux (y compris la sécurité nucléaire, l'intervention en cas de déversement de matières

Terme	Définition
	dangereuses, l'atténuation des effets d'une contamination chimique, biologique, radiologique ou nucléaire, les services de recherche et sauvetage, la sécurité des immeubles, des lieux publics et des rassemblements publics) requis pour maintenir un environnement de maintien de la vie, pour assurer la subsistance et pour protéger la sécurité des personnes, afin d'éviter un préjudice élevé.
Incidence sur la sécurité des Canadiens/du public	Comprend les services essentiels requis pour maintenir l'ordre public, les communications et le transport essentiels, la poursuite des activités du gouvernement, l'intégrité territoriale et la souveraineté de la nation, la sûreté des immeubles, des lieux publics et des rassemblements publics, et la sûreté des Canadiens, afin d'éviter un préjudice élevé.
Incident	Événement susceptible de causer une interruption, une perturbation, une perte, une urgence, une crise, un sinistre ou une catastrophe.
Gestion des incidents	Processus par lequel une organisation intervient et contrôle un incident au moyen de procédures ou de plans d'intervention d'urgence.
Plan d'intervention en cas d'incident	Documentation d'un ensemble prédéterminé d'instructions ou de procédures pour détecter un incident, y réagir et en limiter les conséquences pour les systèmes de TI de l'organisation.
Technologie de l'information (TI)	Utilisation de la technologie pour le stockage, la communication ou le traitement de l'information. La technologie comprend généralement des ordinateurs, des télécommunications, des applications et d'autres logiciels. Les renseignements peuvent inclure des données opérationnelles, de la voix, des images, des vidéos, etc. La technologie de l'information est souvent utilisée pour appuyer les processus opérationnels par l'entremise des services de TI.
Infrastructure comme service (IaaS)	La capacité fournie au consommateur consiste à fournir des services de traitement, de stockage, de réseaux et d'autres ressources informatiques fondamentales permettant au consommateur de déployer et d'exécuter des logiciels arbitraires, notamment des systèmes d'exploitation et des applications. Le consommateur ne gère ni ne contrôle l'infrastructure infonuagique sous-jacente, mais exerce un contrôle sur les systèmes d'exploitation, le stockage et les applications déployées, et peut-être un contrôle limité de certaines composantes de réseautage (p. ex., pare-feu hébergés).
Gestion de la continuité des services de TI (GCSTI)	Processus responsable de la gestion des risques qui pourraient avoir une incidence importante sur les services de TI. Le GCSTI veille à ce que le fournisseur de services de TI puisse toujours fournir des niveaux de service minimaux convenus, en réduisant le risque à un niveau acceptable et en planifiant le rétablissement des services de TI. Le GCSTI devrait être conçu pour appuyer la gestion de la continuité des activités.
Temps d'arrêt maximal acceptable	Temps maximum écoulé entre une interruption et le rétablissement de la capacité opérationnelle requise.
Plateforme comme service (PaaS)	La capacité fournie au consommateur consiste à déployer dans l'infrastructure infonuagique les applications créées ou acquises par le consommateur et créées au moyen de langages de programmation,

Terme	Définition
	de bibliothèques, de services et d'outils soutenus par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure infonuagique sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais il contrôle les applications déployées et peut-être les paramètres de configuration de l'environnement d'hébergement des applications.
Protégé A	Classification canadienne de la confidentialité des données, c'est-à-dire que leur divulgation non autorisée pourrait causer un préjudice, par exemple une atteinte à la vie privée ou de l'embarras.
Protégé B	Classification canadienne de la confidentialité des données, c'est-à-dire que leur divulgation non autorisée pourrait causer un préjudice grave à des intérêts privés ou autres intérêts non nationaux, à une personne ou à une entreprise, comme une atteinte à la vie privée ou un embarras.
RACI	Matrice de propriété des risques, acronyme signifiant Responsable-Imputable-Consulté-Informé
Objectif de point de reprise (OPR)	Point où l'information utilisée par une activité doit être restaurée pour permettre à l'activité de fonctionner à la reprise. Remarque de l'éditeur concernant ISO : On peut aussi parler de « perte maximale de données ».
Objectif de délai de reprise (ODR)	Délai fixé pour le rétablissement et la reprise des fonctions ou des ressources en fonction du temps d'arrêt acceptable et du niveau de rendement acceptable en cas d'interruption des activités.
Région	Une subdivision d'EDSC ventilée selon les frontières géographiques définies par EDSC. Au moment de la rédaction, EDSC comptait cinq régions.
Rapports	Ils comprennent les rapports après action, les journaux d'audit, les rapports de situation, les rapports spéciaux, la liste de vérification des inspections d'étages et les listes de personnes-ressources.
Risque	Événement possible qui pourrait causer des préjudices ou des pertes, ou nuire à la capacité d'atteindre les objectifs. Un risque est mesuré par la probabilité d'une menace, la vulnérabilité de l'actif face à cette menace et l'impact qu'elle produirait s'il survenait.
Évaluation des risques	Processus d'identification des risques pour une organisation, d'évaluation des fonctions essentielles nécessaires à la poursuite des activités opérationnelles, de définition des contrôles en place pour réduire l'exposition de l'organisation et d'évaluation du coût de ces contrôles. L'analyse des risques consiste souvent à évaluer les probabilités d'un événement particulier.
Logiciel en tant que service (SaaS)	La capacité fournie au consommateur consiste à utiliser les applications du fournisseur fonctionnant sur une infrastructure infonuagique. Les applications sont accessibles à partir de divers appareils du client au moyen d'une interface client mince, comme un navigateur Web (p. ex., courriel Web) ou d'une interface de programme. Le consommateur ne gère ni ne contrôle l'infrastructure infonuagique sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même les capacités d'application individuelles, à l'exception peut-être de paramètres limités de configuration d'application spécifiques à l'utilisateur.

Terme	Définition
Mise à l'essai	Activité exécutée pour évaluer l'efficacité ou les capacités d'un plan lié à certains objectifs ou critères de mesure. Elle fait habituellement intervenir des exercices conçus pour maintenir l'efficacité des équipes et employés dans l'exécution de leurs tâches et montrer les faiblesses des plans de préparation et d'intervention, de continuité et de reprise.
Vulnérabilité	Mesure dans laquelle une personne, un actif, un processus, une information, une infrastructure ou d'autres ressources sont exposés aux actions ou aux effets d'un risque, d'un événement ou d'une autre occurrence.

Annexe C – Modèles de services infonuagiques



Le modèle de service infonuagique utilisé dans le cadre de cet approvisionnement est le logiciel en tant que service.

Le modèle de prestation en nuage utilisé dans le cadre de cet approvisionnement est public.
Le consommateur est le gouvernement du Canada.
Le fournisseur de services est un fournisseur du SaaS (c.-à-d. le soumissionnaire).