Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Quebec
K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

Title - Sujet
Système de gestion linguistique

Solicitation No. - N° de l'invitation	**Date**
EN578-170004/B	2018-07-20

Client Reference No. - N° de référence du client
EN578-170004

GETS Reference No. - N° de référence de SEAG
PW-$$EE-006-33702

File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
006ee.EN578-170004	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2019-01-18

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Dhir, Shaveta	006ee

Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 720-9354 ( )	( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Issuing Office - Bureau de distribution
Systems Software Procurement Division / Division des achats des logiciels d'exploitation
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Quebec
K1A 0S5

Canada

DEMANDE DE PROPOSITIONS

POUR LE

SYSTÈME DE GESTION DES DEMANDES DE SERVICES LINGUISTIQUES (SGDSL)

POUR LE

BUREAU DE LA TRADUCTION

DEMANDE DE PROPOSITIONS

SYSTÈME DE GESTION DES DEMANDES DE SERVICES LINGUISTIQUES (SGDSL)

TABLE DES MATIÈRES

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX 4

1.1 INTRODUCTION 4
1.2 SOMMAIRE 4
1.3 VERSIONS MULTIPLES DE LA DP 6
1.4 COMPTE RENDU 6
1.5 AVIS DE COMMUNICATION 7
1.6 CONFLIT D'INTÉRÊTS 7

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES 8

2.1 INSTRUCTIONS, CLAUSES ET CONDITIONS UNIFORMISÉES 8
2.2 PRÉSENTATION DES SOUMISSIONS 8
2.3 ANCIEN FONCTIONNAIRE 8
2.4 DEMANDES DE RENSEIGNEMENTS – EN PÉRIODE DE SOUMISSION 10
2.5 LOIS APPLICABLES 10
2.6 AMÉLIORATIONS APPORTÉES AU BESOIN PENDANT LA DEMANDE DE SOUMISSIONS 10

ANNEXE A ..... ERROR! BOOKMARK NOT DEFINED.

ÉNONCÉ DES TRAVAUX 12

DEMANDE DE PROPOSITIONS

SYSTÈME DE GESTION DES DEMANDES DE SERVICES LINGUISTIQUES (SGDSL)

POUR LE

BUREAU DE LA TRADUCTION

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La demande de soumissions contient sept parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

Partie 1 Renseignements généraux : renferme une description générale du besoin;

Partie 2 Instructions à l'intention des soumissionnaires : renferme les instructions, les clauses et conditions relatives à la demande de soumissions;

Partie 3 Instructions pour la préparation des soumissions : donne aux soumissionnaires les instructions pour préparer leurs soumissions;

Partie 4 Procédures d'évaluation et méthode de sélection : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, ainsi que la méthode de sélection;

Partie 5 Attestations et renseignements supplémentaires : comprend les attestations et les renseignements supplémentaires à fournir;

Partie 6 Exigences relatives à la sécurité, exigences financières et autres exigences : comprend des exigences particulières auxquelles les soumissionnaires doivent répondre;

Partie 7 Clauses du contrat subséquent : contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent.

Les annexes comprennent l'Énoncé des travaux, la Base de paiement, les exigences en matière de sécurité, la Liste de vérification des exigences relatives à la sécurité, les Instruments de paiement électronique, l'attestation du Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation, les exigences en matière d'assurance, le formulaire d'autorisation de tâches (AT) 572 et toutes les autres annexes.

1.2 Sommaire

1.2.1 Travaux publics et Services gouvernementaux Canada (TPSGC) cherche à se procurer, au nom du Bureau de la traduction, un système de gestion des demandes de services linguistiques (SGDSL) sécurisé et complet afin d'assurer la prestation et la gestion des services de traduction et d'interprétation, des processus et des activités de bout en bout et d'une manière intégrée, en ce qui a trait à la classification de sécurité Protégé B des renseignements et des biens classifiés. Il s'agira également de fournir au gouvernement du Canada une capacité en matière de

renseignements d'affaires, ainsi que le soutien et la formation nécessaires à l'excellence du service à la clientèle.

Le Bureau de la traduction est une organisation essentielle pour le gouvernement fédéral : il fournit une multitude de services linguistiques dans trois secteurs d'activités principaux, soit la traduction, la terminologie et l'interprétation à des clients internes et externes, dont le Parlement, les tribunaux, les ministères et les organismes fédéraux ainsi que le milieu universitaire. Le Bureau de la traduction constitue également l'autorité du gouvernement du Canada (GC) en matière de terminologie et a reçu le mandat d'élaborer des normes terminologiques pour garantir des communications claires, uniformes et de qualité au sein du gouvernement.

La solution du SGDSL doit être un service géré par l'entrepreneur, qui permet d'utiliser les applications du fournisseur hébergées dans l'infrastructure de ce dernier ou de son sous-traitant. Elle doit être sécurisée, fonctionnelle, complète, ainsi qu'exempte de bogues et entièrement hébergée au Canada, y compris les centres de données de l'entrepreneur ou de son sous-traitant, l'infrastructure de service sous-jacente, le réseau, les bases de données, les serveurs Web, les applications, les systèmes d'exploitation, les machines virtuelles ainsi que le stockage de données.

L'entrepreneur doit héberger, livrer, configurer, mettre à l'essai, mettre en œuvre, appuyer et gérer une solution de SGDSL en français et en anglais pour le compte du Bureau de la traduction, ainsi que s'assurer de sa compatibilité avec ses systèmes.

Les fonctions de base de la solution de SGDSL doivent comprendre ce qui suit :

a) des portails pour les ressources et les clients du Bureau de la traduction, ainsi que pour ses fournisseurs de services linguistiques externes;
b) la gestion du flux de travail;
c) la gestion de la charge de travail;
d) la gestion de la terminologie;
e) des outils de traduction assistée par ordinateur (TAO);
f) des outils d'assurance de la qualité;
g) une solution d'analyse, de production de rapports et de vérification;
h) l'interopérabilité de la gestion financière;
i) la gestion de la sécurité;
j) la gestion de l'adaptabilité;
k) la gestion des documents.

1.2.2 Ce besoin comporte des exigences relatives à la sécurité. Pour de plus amples renseignements, consulter la Partie 6, Exigences relatives à la sécurité, exigences financières et autres exigences, et la Partie 7, Clauses du contrat subséquent. Pour de plus amples renseignements sur les enquêtes de sécurité sur le personnel et les organismes, les soumissionnaires devraient consulter le site Web du Programme de sécurité des contrats de Travaux publics et Services gouvernementaux Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

1.2.3 Le besoin est assujetti aux dispositions de l'Accord sur les marchés publics de l'Organisation mondiale du commerce (AMP-OMC), de l'Accord de libre-échange nord-américain (ALENA), de l'Accord économique et commercial global entre le Canada et l'Union européenne (AECG) et de l'Accord de libre-échange canadien (ALEC).

1.2.4 La présente demande de soumissions vise à établir un contrat comportant des AT pour répondre au besoin décrit dans la demande de soumissions aux utilisateurs désignés, et ce, partout au

Canada, sauf dans les zones visées par des ententes sur les revendications territoriales globales au Yukon, dans les Territoires du Nord-Ouest, au Nunavut, au Québec et au Labrador. Les exigences relatives aux produits à livrer dans les zones visées par des ERTG au Yukon, dans les Territoires du Nord-Ouest, au Nunavut, au Québec et au Labrador devront faire l'objet de contrats distincts, attribués en dehors du contrat subséquent.

1.2.5 Le PCF s'applique au présent besoin (voir la partie 5, Attestations et renseignements supplémentaires, la partie 7, Clauses du contrat subséquent, et l'annexe intitulée Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation.

1.2.6 Les soumissionnaires peuvent utiliser le service Connexion postel de la Société canadienne des postes pour présenter leur soumission. Les soumissionnaires doivent se reporter à la partie 2 de la demande de soumissions, Instructions à l'intention des soumissionnaires, pour obtenir de l'information supplémentaire.

1.3. Versions multiples de la DP

1.3.1 Le Canada publiera sous peu une demande de propositions (DP) pour un système de gestion des demandes de services linguistiques (SGDSL) en trois versions distinctes, qui seront toutefois associées à une seule date de clôture des soumissions. Il s'agira de donner au soumissionnaire un préavis suffisant lui permettant de commencer à préparer sa soumission, comme il sera décrit dans la demande de soumissions.

Voici une description du contenu de chacune des versions de la DP :

<u>Première version de la DP</u> :

- Partie 1 de la DP – Renseignements généraux;
- Partie 2 de la DP – Instructions à l'intention des soumissionnaires;
- Annexe A – Énoncé des travaux (EDT);

<u>Deuxième version de la DP</u> :

- Partie 7 de la DP – Clauses du contrat subséquent

<u>Troisième version de la DP</u> :

- Partie 3 de la DP – Instructions pour la préparation des soumissions;
- Partie 4 de la DP – Procédures d'évaluation et méthode de sélection;
- Partie 5 de la DP – Attestations;
- Partie 6 de la DP – Exigences relatives à la sécurité et exigences financières;
- Plan d'évaluation et méthodologie.

Le Canada se réserve le droit, à sa seule discrétion, de modifier la séquence, le contenu et les dates des versions de la DP; ainsi que le nombre de versions liées à la présente DP.

1.4. Compte rendu

1.4.1 Les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Ils devraient en faire la demande à l'autorité contractante dans les

15 jours ouvrables suivant la réception des résultats du processus de demande de soumissions. Le compte rendu peut être fourni par écrit, par téléphone ou en personne.

L'autorité contractante pour la demande de soumissions est :

Nom : Shaveta Dhir
Titre : Spécialiste en approvisionnement
Organisation : Services publics et Approvisionnement Canada
Adresse : 10, rue Wellington, 4e étage
Gatineau (Québec) K1A 0S5
Téléphone : 613-720-9354
Adresse de courriel: shaveta.dhir@tpsgc-pwgsc.gc.ca

1.5. Avis de communication

1.5.1 À titre de courtoisie, le GC demande aux soumissionnaires retenus d'aviser au préalable l'autorité contractante de leur intention de rendre publique une annonce relative à l'attribution d'un contrat.

1.6. Conflit d'intérêts

1.6.1 On recommande aux soumissionnaires de se référer aux dispositions relatives aux conflits d'intérêts à la section 18 du Guide des clauses et conditions uniformisées d'achat (CCUA) 2003, Instructions uniformisées – biens ou services – besoins concurrentiels (datées du 22-05-2018) et aux dispositions relatives aux conflits d'intérêts du Guide des CCUA 2035, conditions générales – besoins plus complexes – services (datées du 21-06-2018) publié sur le site Web de TPSGC, à l'adresse : https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat.

1.6.2 Sans limiter d'aucune façon les dispositions décrites au paragraphe 1.6.1 ci-dessus, les soumissionnaires sont priés de noter que le Canada a fait appel aux ressources entrepreneurs et aux ressources suivants du secteur privé, qui ont assuré la prestation de certains services, à savoir l'examen du contenu dans le cadre de la préparation de la présente DP. Ces personnes ont eu ou pourraient avoir accès aux renseignements relatifs au contenu de la DP ou à d'autres documents ayant trait à la demande de soumissions pour le SGDSL :

S. I Systems Pièce 350 160, avenue Carling Ottawa (Ontario) K1Z 1G3
IBISKA 1500-130, rue Albert, Ottawa (Ontario) K1P 5G4
CGI Information Systems and Management Consultants Inc. 1410 Blair Place, 6e étage, Ottawa (Ontario) K1J 9B9

TRM Technologies
280, rue Albert,
Ottawa (Ontario) K1P 5G8

Toute soumission reçue de l'un des fournisseurs mentionnés ci-dessus, qu'il soit un soumissionnaire unique, une coentreprise ou le sous-traitant d'un soumissionnaire, ou toute soumission à laquelle l'une des ressources susmentionnées a contribué dans la soumission sera considérée comme étant en infraction aux dispositions relatives au conflit d'intérêts mentionnées au paragraphe 1.6.1 et sera déclarée non recevable.

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

2.1.1 Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions par un numéro, une date et un titre sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Travaux publics et Services gouvernementaux Canada.

2.1.2 Les soumissionnaires qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions, et acceptent les clauses et les conditions du contrat subséquent.

2.1.3 Les Instructions uniformisées 2003 (22-05-2018) – biens ou services – besoins concurrentiels, sont incorporées par renvoi dans la demande de soumissions et en font partie intégrante.

2.1.4 Le paragraphe 5 des Instructions uniformisées 2003 (22-05-2018) – biens ou services – besoins concurrentiels, est modifié comme suit :

Supprimer : 60 jours
Insérer : 200 jours

2.2 Présentation des soumissions

2.2.1 Les soumissions doivent être présentées au Module de réception des soumissions de Travaux publics et Services gouvernementaux Canada (TPSGC) au plus tard à la date, à l'heure et à l'endroit indiqués dans la demande de soumissions.

2.2.2 Sauf indication contraire dans la demande de soumissions, les soumissions peuvent être transmises par télécopieur. Le seul numéro de télécopieur valide pour la réception des réponses aux demandes de soumissions émises par l'administration centrale de TPSGC est le 819-997-9776.

2.2.3 À moins d'indication contraire dans la demande de soumissions, les soumissions peuvent être transmises à l'aide du service Connexion postel de la Société canadienne des postes. La seule adresse courriel valide pour transmettre les réponses aux demandes de soumissions émises par l'administration centrale de TPSGC à l'aide du service Connexion postel est : tpsgc.dgareceptiondessoumissions-abbidReceiving.pwgsc@tpsgc-pwgsc.gc.ca .

2.3 Ancien fonctionnaire

Les contrats attribués à d'anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen scrupuleux du public et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du Trésor sur les contrats attribués à d'anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée ci-dessous avant l'attribution du contrat. Si les réponses aux questions et, selon les cas, les renseignements requis n'ont pas été fournis à la date de fin de l'évaluation des soumissions, le Canada informera le soumissionnaire du délai imparti pour fournir les renseignements. Le défaut de répondre à la demande du Canada et de se conformer aux exigences dans les délais prévus aura pour conséquence de rendre la soumission irrecevable.

Définitions

Aux fins de la présente clause, « ancien fonctionnaire » désigne un ancien employé d'un ministère au sens de la *Loi sur la gestion des finances publiques*, L.R., 1985, ch. F-11, un ancien membre des Forces armées canadiennes ou un ancien membre de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être :

a. une personne;
b. une personne morale;
c. une société de personnes constituée d'anciens fonctionnaires; ou
d. une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.

« période du paiement forfaitaire » signifie la période mesurée en semaines de salaire à l'égard de laquelle un paiement a été fait pour faciliter la transition vers la retraite ou vers un autre emploi par suite de la mise en place des divers programmes visant à réduire la taille de la fonction publique. La période du paiement forfaitaire ne comprend pas la période visée par l'indemnité de départ, qui se mesure de façon similaire.

« pension » signifie, une pension ou une allocation annuelle versée en vertu de la *Loi sur la pension de la fonction publique (LPFP)* (PSSA), L.R., 1985, cf. P-36, et toute augmentation versée en vertu de la *Loi sur les prestations de retraite supplémentaires*, L.R., 1985, ch. S-24, dans la mesure où elle touche la LPFP. La pension ne comprend pas les pensions payables conformément à la *Loi sur la pension de retraite des Forces canadiennes*, L.R., 1985, ch. C-17, à la *Loi sur la continuation de la pension des services de défense*, 1970, ch. D-3, à la *Loi sur la continuation des pensions de la Gendarmerie royale du Canada* , 1970, ch. R-10, à la *Loi sur la pension de retraite de la Gendarmerie royale du Canada*, L.R., 1985, ch. R-11, à la *Loi sur les allocations de retraite des parlemenetaires*, L.R. 1985, ch. M-5, et à la partie de la pension versée conformément au *Régime de pensions du Canada*, L.R., 1985, ch. C-8.

Ancien fonctionnaire touchant une pension

Selon les définitions ci-dessus, est-ce que le soumissionnaire est un ancien fonctionnaire touchant une pension? **Oui** ( ) **Non** ( )

Si oui, le soumissionnaire doit fournir les renseignements suivants pour les anciens fonctionnaires touchant une pension :

a. le nom de l'ancien fonctionnaire;
b. la date de cessation d'emploi dans la fonction publique ou du départ à la retraite de la fonction publique.

En fournissant cette information, les soumissionnaires acceptent que le statut du soumissionnaire retenu, en tant qu'ancien fonctionnaire touchant une pension en vertu de la LPFP, soit publié dans les rapports de divulgation proactive des marchés, sur les sites Web des ministères, et ce conformément à l'Avis sur la Politique des marchés : 2012-2 et aux Lignes directrices sur la divulgation proactive des marchés.

Directive sur le réaménagement des effectifs

Le soumissionnaire est-il un ancien fonctionnaire qui a touché un paiement forfaitaire conformément aux modalités de la Directive sur le réaménagement des effectifs? **Oui** ( ) **Non** ( )

Si oui, le soumissionnaire doit fournir l'information suivante :

a. le nom de l'ancien fonctionnaire;
b. les conditions de l'incitatif versé sous forme de paiement forfaitaire;
c. la date de la cessation d'emploi;
d. le montant du paiement forfaitaire;
e. le taux de rémunération qui a servi au calcul du paiement forfaitaire;
f. la période du paiement forfaitaire, y compris la date de début, la date de fin et le nombre de semaines;
g. le nombre et le montant (honoraires professionnels) des autres contrats assujettis aux conditions d'un programme de réaménagement des effectifs.

Pour tous les contrats attribués pendant la période du paiement forfaitaire, le montant total des honoraires qui peut être payé à un ancien fonctionnaire qui a reçu un paiement forfaitaire est limité à 5 000 $, incluant les taxes applicables.

2.4 Demandes de renseignements – en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins 10 jours civils avant la date de clôture des soumissions. Il se pourrait que l'on ne puisse pas répondre aux demandes de renseignements reçues après ce délai.

Les soumissionnaires devraient indiquer aussi fidèlement que possible l'article numéroté de la demande de soumissions auquel se rapporte leur demande de renseignements. Ils doivent prendre soin d'expliquer chaque question en donnant suffisamment de détails pour permettre au Canada de fournir une réponse exacte. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le gouvernement du Canada peut réviser les questions ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permettrait pas de les diffuser à tous les soumissionnaires.

2.5 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur en Ontario, et les relations entre les parties seront déterminées par ces lois.

À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province

ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées.

2.6 Améliorations apportées au besoin pendant la demande de soumissions

Les soumissionnaires qui estiment qu'ils peuvent améliorer, techniquement ou technologiq Améliorations apportées au besoin pendant la demande de soumissions uement, le devis descriptif ou l'Énoncé des travaux contenus dans la demande de soumissions, sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la demande de soumissions. Les soumissionnaires doivent indiquer clairement les améliorations suggérées et les motifs qui les justifient. Les suggestions qui ne restreignent pas la concurrence ou qui ne favorisent pas un soumissionnaire en particulier seront examinées à la condition qu’elles parviennent à l’autorité contractante au plus tard 15 jours avant la date de clôture de la demande de soumissions. Le Canada aura le droit d’accepter ou de rejeter n’importe laquelle ou la totalité des suggestions proposées.

ANNEXE A

ÉNONCÉ DES TRAVAUX

Système de gestion des demandes de services linguistiques (SGDSL)

TABLE DES MATIÈRES

1. SYSTÈME DE GESTION DES DEMANDES DE SERVICES LINGUISTIQUES (SGDSL) 7
1.1 RÉSUMÉ 7
1.2 CONTEXTE 8
1.3 PORTÉE DES TRAVAUX 10
1.3.1 Vision et approche visant le déploiement de la *solution de SGDSL* 12
1.4 STRUCTURE DE L'ÉNONCÉ DES TRAVAUX 13
1.5 TERMINOLOGIE COMMUNE 14
1.6 BUREAU DE LA TRADUCTION 14
1.6.1 Aperçu 14
1.7 DONNÉES VOLUMÉTRIQUES 15
1.8 SECTEURS, FONCTIONS OPÉRATIONNELLES ET ACTIVITÉS CLÉS DU BUREAU DE LA TRADUCTION17
1.9 SERVICES DU BUREAU DE LA TRADUCTION 19
1.10 FLUX DE TRAVAUX DU BUREAU DE LA TRADUCTION 21
1.10.1 Aperçu 21
1.10.2 Flux de travaux de traduction 22
2 exigences relatives aux lois, aux règlements et aux politiques 25
2.1 INTRODUCTION 25
2.2 LOIS, REGLEMENTS, POLITIQUES, DIRECTIVES, NORMES ET LIGNES DIRECTRICES 25
3 EXIGENCES FONCTIONNELLES 27
3.1 INTRODUCTION AUX EXIGENCES FONCTIONNELLES 27
3.2 SECTION A – EXIGENCES GÉNÉRALES 27
3.2.1 Objectif 27
3.2.2 Exigences 27
3.3 SECTION B – EXIGENCES LINGUISTIQUES 31
3.3.1 Objectif 32
3.3.2 Exigences 32
3.4 SECTION C – EXIGENCES DU PORTAIL 33
3.4.1 Objectif 33
3.4.2 Exigences 33
3.5 SECTION D – GESTION DU FLUX DE TRAVAUX 36
3.5.1 Objectif 36
3.5.2 Exigences 37
3.6 SECTION E – GESTION DE LA CHARGE DE TRAVAIL 38
3.6.1 Objectifs 38
3.6.2 Exigences 38
3.7 SECTION F – TRADUCTION ASSISTÉE PAR ORDINATEUR (TAO) 42
3.7.1 Objectifs 42
3.7.2 Aperçu 42
3.8 SECTION G – ANALYSES, RAPPORTS ET VÉRIFICATIONS 54
3.8.1 Objectifs 54
3.8.2 Exigences 54
3.9 SECTION H – GESTION DES DONNÉES ET DE L'INFORMATION 58

3.9.1 Objectif ... 58
3.9.2 Exigences ... 59
3.10 SECTION I – GESTION DES UTILISATEURS ... 61
3.10.1 Objectif ... 61
3.10.2 Exigences en matière de gestion des utilisateurs et produits livrables ... 61
3.10.3 Exigences ... 61
4 EXIGENCES TECHNIQUES ... 64
4.1 TECHNOLOGIE DE L'INFORMATION, ET MAINTENANCE ET MISE À JOUR DE LA SOLUTION ... 64
4.1.1 Solution hébergée – SGDSL ... 64
4.2 EXIGENCES RELATIVES AU MATÉRIEL ... 64
4.3 INTEROPÉRABILITÉ AVEC LES AUTRES SYSTÈMES ET ENVIRONNEMENTS ... 64
4.3.1 Contexte ... 64
4.3.2 Interopérabilité générale du système ... 65
4.3.3 Interopérabilité technique ... 66
4.3.4 Exigences ... 66
4.4 EXIGENCES TECHNOLOGIQUES DU SGDSL ... 67
4.4.1 Introduction ... 67
4.4.2 Conformité ... 67
4.4.3 Interopérabilité ... 67
4.4.4 Convivialité ... 67
4.4.5 Fiabilité ... 67
4.4.6 Adaptabilité ... 67
4.4.7 Exigences ... 68
5 EXIGENCES NON FONCTIONNELLES ... 72
5.1 CONTEXTE ... 72
5.2 ENGAGEMENTS GÉNÉRAUX ... 72
5.2.1 Adaptation aux changements ... 72
5.2.2 Souplesse de la solution ... 72
5.2.3 Convivialité de la solution ... 73
5.2.4 Principes de gestion efficace de l'information ... 73
5.3 EXIGENCES EN MATIÈRES DE SÉCURITÉ ... 74
5.3.1 Sécurité ... 74
5.3.2 Renseignements personnels ... 74
5.3.3 Renseignements protégés ... 74
5.3.4 Programme d'évaluation et d'autorisation de sécurité et conformité en la matière ... 75
5.3.5 Gestion des risques ... 75
5.3.6 Contrôle d'accès ... 75
5.3.7 Information, données et services de la solution du SGDSL ... 76
5.3.8 Divulgation ... 76
5.3.9 Chiffrement ... 76
5.3.10 Fuite de données ... 76
5.3.11 Fonctionnalité minimale ... 77
5.3.12 Réponse en cas d'incident ... 77
5.3.13 Vérification ... 77

5.3.14 Profil de contrôle de sécurité (PCS) 78
5.3.15 Éléments de preuve 78
5.3.16 Attestations de sécurité de la TI 78
5.3.17 Exigences 79
5.4 GESTION DES SERVICES 82
5.4.1 Contexte 82
5.4.2 Service de gestion des services de TI : gestion des incidents, des problèmes, des changements et des versions 83
5.4.3 Exigences relatives aux niveaux de service 84
5.4.4 Normes de service 85
5.4.5 Bureau de service 87
5.5 ACCESSIBILITÉ WEB 96
5.5.1 Accessibilité Web 96
5.5.2 Exigences de conformité relatives aux contenus Web 2.0 97
6 Gestion et surveillance 98
6.1 CONTEXTE 98
6.2 ATTENTES EN MATIÈRE DE GOUVERNANCE – MÉTHODE DE GESTION 98
6.2.1 Principes de gestion et de gouvernance 98
6.2.2 Principes de planification 98
6.3 PLANS DE PROJET 99
6.3.1 Plan de gestion de projet 99
6.4 GESTION DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 101
6.4.1 Plan de gestion de la protection des renseignements personnels 101
6.4.2 Mise en œuvre du plan de gestion de la protection des renseignements personnels 102
6.4.3 Évaluation des facteurs relatifs à la vie privée 102
6.5 GESTION DE LA SÉCURITÉ DES TI 103
6.5.1 Centre des opérations de protection des TI 103
6.5.2 Plan de sécurité des TI 104
6.5.3 Plan de continuité des services et de reprise après sinistre 104
6.5.4 Schémas de l'architecture technique 104
6.5.5 Approche relative à l'intégration technique 104
6.6 PROCESSUS D'ÉVALUATION ET D'AUTORISATION DE SÉCURITÉ DE SPAC 104
6.6.1 Point de contrôle 1 du processus d'évaluation et d'autorisation de sécurité 105
6.6.2 Point de contrôle 2 du processus d'évaluation et d'autorisation de sécurité 106
6.6.3 Point de contrôle 3 du processus d'évaluation et d'autorisation de sécurité 108
6.7 SERVICES DE TRANSITION 110
6.7.1 Services de transition d'entrée 110
6.7.2 Services de soutien continu 115
6.7.3 Entretien 115
6.7.4 Services de transition de sortie 116
6.8 RÉUNIONS ET RAPPORTS 118
6.8.1 Réunion de lancement 118
6.8.2 Réunions d'étape hebdomadaires 119
6.8.3 Rapport mensuel sur l'avancement du projet 119

6.8.4 Examens semestriels concernant la gestion stratégique 119
6.9 SOMMAIRE DES PRODUITS LIVRABLES 120
6.10 CADRE SUR L'ACCEPTATION DES PRODUITS LIVRABLES 122
6.10.1 Cadre sur l'acceptation des produits livrables 122
6.10.2 Acceptation ou rejet des produits livrables 123
6.10.3 Soumettre de nouveau un produit livrable rejeté 123
6.10.4 Processus de soumission des produits livrables 123
6.11 PLAN DE CONTINUITÉ DES SERVICES ET DE REPRISE APRÈS SINISTRE 123
6.11.1 Contexte 123
6.11.2 Plan de continuité des services 124
6.11.3 Plan de reprise après sinistre 124
6.11.4 Exigences 125
6.12 PLAN DE MIGRATION DES DONNÉES 126
6.12.1 Contexte 126
6.12.2 Migration des données 126
6.13 FORMATION, TRANSFERT DES CONNAISSANCES ET DOCUMENTATION 128
6.13.1 Contexte 128
6.13.2 Formation et transfert des connaissances 128
6.13.3 Documentation 129
6.13.4 Exigences 130
6.14 GESTION DES CHANGEMENTS 131
6.14.1 Contexte 131
6.14.2 Objectif 132
6.14.3 Approche 132
6.14.4 Demandes de changement 133
6.14.5 Prestation 134
6.14.6 Exigences 135
6.15 GESTION DES VERSIONS 136
6.15.1 Contexte 136
6.15.2 Gestion des versions 137
7 SERVICES PROFESSIONNELS 139
7.1 SERVICES PROFESSIONNELS 139
7.1.1 Services supplémentaires de gestion du changement et de soutien à la transformation des activités 139
7.2 TRAVAUX ADDITIONNELS 139
7.2.1 Configuration supplémentaire du système 139
7.2.2 Migration des anciennes données 140
7.2.3 Intégration d'un tiers 140
7.2.4 Accès aux données 140
8 APPENDICE A – GLOSSAIRE 141
9 APPENDICE B – ACRONYMES 163
10 APPENDICE C – RAPPORTS DU BUREAU DE LA TRADUCTION 167
11 APPENDICE D – RESPONSABILITÉ DES RESSOURCES EN SERVICES PROFESSIONNELS 169

12 APPENDICE E – CALCUL DE LA CHARGE DE TRAVAIL D'INTERPRÉTATION ET EXEMPLE 172
12.1 HEURES DE TRAVAIL – INTERPRÈTES 172
12.2 EXEMPLE DE CALCUL – HEURES DE TRAVAIL – INTERPRÈTES 174
13 APPENDICE F – LANGUES ET FORMATS DE FICHIERS DU BUREAU DE LA TRADUCTION 175
13.1 LANGUES 175
13.2 FORMATS DE FICHIERS 177
14 APPENDICE G – SÉCURITÉ ET PROTECTION DES renseignements PERSONNELS 179
14.1 FAMILLES DE CONTRÔLES SELON L'ITSG-33 179
14.1.1 Contrôles de sécurité de l'ITSG-33 appliqués au SGDSL 179
14.1.2 Contrôles de sécurité de l'industrie pour La solution SGDSL 228
14.2 MATRICE DE TRAÇABILITÉ DES EXIGENCES RELATIVES À LA SÉCURITÉ (MTERS) 240
14.2.1 Conformité aux contrôles de sécurité : éléments de preuve acceptables 240
14.2.2 Politiques, normes et lignes directrices 240
14.2.3 Certification et autorisations 240
14.2.4 Exemples d'éléments de preuve 240
14.2.5 Exemple de matrice de traçabilité des exigences relatives à la sécurité 241

1. SYSTÈME DE GESTION DES DEMANDES DE SERVICES LINGUISTIQUES (SGDSL)

1.1 RÉSUMÉ

L'entrepreneur doit fournir au Bureau de la traduction de Services publics et Approvisionnement Canada (SPAC), un système de gestion des demandes de services linguistiques (ci-après appelé ***solution de SGDSL***) bilingue (français et anglais) qu'il doit héberger, configurer, mettre à l'essai, mettre en œuvre, prendre en charge et gérer, en plus d'en assurer l'interopérabilité.

La ***solution de SGDSL*** doit être un service géré par l'entrepreneur qui utilise des applications du fournisseur hébergées dans l'infrastructure de l'entrepreneur ou d'un sous-traitant, qui est sécurisé, opérationnel, complet et exempt de bogues, qui est entièrement hébergé au Canada et qui comprend des centres de données, l'infrastructure de service sous-jacente, un réseau, une base de données, le Web, des serveurs d'application, des systèmes d'exploitation, des machines virtuelles et des dispositifs de stockage de l'entrepreneur ou d'un sous-traitant.

Toutes les données et l'information qui sont transférées, archivées, sauvegardées, stockées sur des supports ou créées dans la ***solution de SGDSL***, ou qui y sont associées, seront conservées au Canada et demeureront la propriété du Canada en tout temps. Par conséquent, elles devront être chiffrées dans le respect des exigences de sécurité du gouvernement du Canada (ci-après GC). Les données doivent demeurer dans leur format d'origine. Ce format ne doit pas être converti en un format exclusif, car le GC doit être en mesure d'accéder à ses données en tout temps.

La ***solution de SGDSL*** fournie au **client** par l'entrepreneur doit utiliser des applications fonctionnant dans l'infrastructure de service géré par l'entrepreneur et être sécurisée, basée sur le Web et accessible à partir des appareils des clients du Bureau de la traduction au moyen d'un navigateur Web pris en charge par le GC. Il n'est pas nécessaire que les caractéristiques et les fonctionnalités soient comprises initialement dans une application; cependant, l'entrepreneur doit veiller à ce que les applications soient harmonieusement intégrées.

L'entrepreneur doit configurer la ***solution de SGDSL*** de façon à assurer le respect des exigences relatives aux lois, aux règlements et aux politiques du GC, comme l'indique la partie 2.

La ***solution de SGDSL*** doit pouvoir interagir avec d'autres systèmes et outils qui seront déterminés par SPAC en collaboration avec l'entrepreneur.

L'entrepreneur doit déployer une ***solution de SGDSL*** qui est flexible, évolutive et adaptable, ce qui se traduira par des coûts d'amélioration minimes pour le Bureau de la traduction de SPAC en ce qui a trait à l'adaptation et au déploiement. La conception, la configuration, l'élaboration et la mise en œuvre de la ***solution de SGDSL*** doivent faire l'objet d'une surveillance adéquate de la part du **client** afin de faire en sorte que l'entrepreneur respecte l'échéancier et que la ***solution de SGDSL*** soit conforme aux exigences du Bureau de la traduction de SPAC, comme l'indique l'énoncé des travaux (EDT).

La ***solution de SGDSL*** doit offrir les caractéristiques et les fonctionnalités nécessaires pour exécuter et gérer les services, les processus, les tâches et les activités de traduction, de terminologie et d'interprétation de bout en bout du Bureau de la traduction de SPAC à l'appui des demandes de service des clients comportant une cote de sécurité du GC jusqu'au niveau Protégé B (se reporter à l'*appendice A – Glossaire* pour obtenir les niveaux de classification de sécurité du GC).

La ***solution de SGDSL*** doit être conforme (pour plus de renseignements, se reporter à la *section 1.3 – Portée des travaux*) :

a) aux exigences relatives aux langues officielles du Canada;
b) aux normes de sécurité et aux profils de contrôle de sécurité en matière de TI du GC.

Voici les fonctionnalités de base de la ***solution de SGDSL*** à inclure (pour plus de renseignements, se reporter à la *section 1.3 – Portée des travaux*) :

a) portails pour les ressources, les clients et les fournisseurs de services linguistiques externes du Bureau de la traduction;
b) gestion des flux de travaux;
c) gestion de la charge de travail;
d) gestion de la terminologie;
e) outils de traduction assistée par ordinateur (TAO);
f) outils d'assurance de la qualité;
g) analyses, production de rapports et vérification;
h) interopérabilité avec les systèmes de gestion financière;
i) gestion de la sécurité;
j) gestion de l'adaptabilité;
k) gestion des documents.

De plus, l'entrepreneur devra établir et conserver un bureau de service francophone et anglophone situé au Canada (pour plus de renseignements, se reporter à la section 5.5) pour répondre aux demandes de soutien technique du Bureau de la traduction de SPAC. L'entrepreneur sera le seul point de contact pour toutes les questions touchant la ***solution de SGDSL***, y compris celles liées au sous-traitant.

L'entrepreneur doit aussi fournir les documents, les plans, les évaluations de sécurité et les rapports comme il est décrit dans le présent EDT.

1.2 CONTEXTE

Le Bureau de la traduction est essentiel pour le gouvernement fédéral puisqu'il fournit une gamme de services linguistiques à l'échelle de trois secteurs d'activités (traduction, terminologie et interprétation) à des clients internes et externes du Bureau de la traduction, au Parlement, à l'appareil judiciaire, aux ministères et organismes fédéraux, et au milieu universitaire. Il s'agit également de l'autorité en matière de terminologie au sein du GC et, à cet égard, il a été chargé d'uniformiser la terminologie afin d'assurer des communications claires, cohérentes et de qualité au sein du gouvernement. Le programme de services et de gestion linguistiques tire son mandat de la *Loi sur le Bureau de la traduction*. De plus, le Bureau de la traduction mène ses activités dans un environnement financier complexe : fonds renouvelables, crédits et affectation à but spécial.

Le Bureau de la traduction gère et fournit des services de traduction de plus de 350 millions de mots pour le compte de ministères et d'organismes, de plus de 44 millions de mots pour le Parlement, ce qui représente approximativement 75 % des dépenses totales pour le GC. Le Bureau de la traduction fournit également des services d'interprétation pour plus de 5000 jours/interprète dans le cadre de réunions parlementaires et 7000 jours/interprète dans le cadre de conférences.

Le Bureau de la traduction garantit à ses clients des produits de qualité et, ainsi, applique des processus de contrôle de la qualité rigoureux, y compris de la révision et de la correction d'épreuves. Pour fournir ses services, le Bureau de la traduction compte sur un vaste bassin de traducteurs, d'interprètes et de terminologues internes et externes, appuyés par un réseau complexe de ressources spécialisées, comme des techniciens en éditique, des bibliotechniciens de référence, des agents d'appui professionnel, des commis de gestion des dossiers, des analystes d'affaires et des formateurs.

Le Bureau de la traduction utilise actuellement une combinaison d'outils internes et commerciaux autonomes pour gérer et exécuter les travaux, et en assurer le suivi. La technologie actuelle prenant en charge ces fonctions est désuète. Elle n'est plus viable ni adaptable, et sa prise en charge est très coûteuse. Le flux de travaux actuel nécessite trop d'interventions manuelles, ce qui nuit à l'efficacité et entraîne des risques d'erreurs plus élevés. Du point de vue des clients du Bureau de la traduction, le Bureau fonctionne en tout temps et, ainsi, il est plus difficile de desservir les clients du Bureau de la traduction sans un modèle libre-service ou des fonctions automatisées. Les ***fournisseurs*** (interprètes et traducteurs fournisseurs de services linguistiques) n'ont actuellement pas accès aux systèmes du Bureau. Les communications entre le Bureau de la traduction et les ***fournisseurs*** se font par courriel, ce qui crée inutilement un volume élevé de trafic. Les traductions et les documents de référence sont dispersés et ne sont pas stockés dans un emplacement central, ce qui rend encore plus difficile d'assurer la cohérence et la qualité.

Afin d'optimiser le portefeuille d'applications de SPAC et de réduire les coûts de soutien et de maintenance connexes, l'architecture de référence de SPAC présente des solutions ciblées pour répondre aux exigences opérationnelles clés. La ***solution de SGDSL*** est la solution commerciale ciblée pour répondre aux exigences en matière d'automatisation des processus opérationnels et de gestion des relations avec la clientèle du Bureau de la traduction. Elle vise à atteindre les résultats suivants :

a) normaliser et rationaliser les processus opérationnels;

b) être harmonisée aux pratiques exemplaires de l'industrie en matière de gestion de la traduction, de l'interprétation et de la terminologie;

c) simplifier et moderniser l'offre de services en tirant parti de la technologie pour faciliter les tâches quotidiennes et accroître l'efficience;

d) permettre la prise en charge électronique (fourniture d'un service qui peut être offert en ligne de bout en bout, à l'exception de circonstances où c'est interdit par la loi ou lorsque des considérations liées à la sécurité pour les services l'exigent) pour les principaux points d'interaction avec les clients du Bureau de la traduction : inscription, authentification, application, décision, prestation de services et résolution de problèmes/rétroaction (se reporter à la Politique sur les services);

e) optimiser et automatiser la gestion des demandes pour mieux attribuer la charge de travail, accroître la productivité et améliorer l'utilisation des ressources internes et externes pour l'exécution des travaux;

f) automatiser la facturation des clients du Bureau de la traduction pour les travaux exécutés ainsi que le paiement des pigistes pour les services rendus, et assurer le suivi et la production de rapports à cet égard;

g) offrir une certaine souplesse pour élargir la portée des besoins et répondre aux besoins supplémentaires, en plus de réduire davantage le nombre d'applications vieillissantes.

1.3 PORTÉE DES TRAVAUX

La portée du projet vise l'hébergement, la livraison, la configuration, la mise à l'essai, la mise en œuvre, l'interopérabilité, le soutien et la gestion d'un service géré par l'entrepreneur qui utilise des applications du fournisseur hébergées dans l'infrastructure de l'entrepreneur ou d'un sous-traitant et qui répond à un besoin pour un système de gestion des demandes de services linguistiques (SGDSL) disponible en français et en anglais. Cela comprendra activer toutes les composantes de la ***solution de SGDSL*** qui auront fait l'objet d'un ensemble exhaustif d'essais d'acceptation par les utilisateurs des secteurs d'activités, d'un projet pilote auprès d'un groupe d'utilisateurs établi ainsi que d'une mise en service suivie d'un lancement complet ou graduel, qui pourrait également comprendre une utilisation simultanée de l'ancien système et de la nouvelle ***solution de SGDSL*** pendant un certain temps et être déterminé par SPAC en collaboration avec l'entrepreneur.

Ce projet comprend des activités de gestion de projet, des évaluations de sécurité, le transfert de données, la continuité des activités et la reprise après sinistre, la maintenance, le soutien et la formation. Le Bureau de la traduction exigera un soutien en français et en anglais de l'entrepreneur et ce dernier pourrait être appelé à fournir des services professionnels sur demande par l'entremise d'autorisations de tâches dans le cadre du contrat.

La ***solution de SGDSL*** doit être conforme aux lois et aux normes du GC :

a) ***Langues officielles du Canada*** : Doit être conforme à la Loi sur les langues officielles du Canada et permettre à l'utilisateur d'utiliser le système dans la langue de son choix (français ou anglais).

b) **Sécurité du GC** : Doit être conforme aux lignes directrices de sécurité et aux profils de contrôle de sécurité en matière de TI du GC.

La ***solution de SGDSL*** doit être conforme aux exigences suivantes :

c) Service géré par l'entrepreneur : La ***solution de SGDSL*** doit être un service géré par l'entrepreneur qui utilise des applications du fournisseur hébergées dans l'infrastructure de l'entrepreneur ou d'un sous-traitant, qui est sécurisé, opérationnel, complet et exempt de bogues, est entièrement hébergé au Canada et comprend des centres de données, l'infrastructure de service sous-jacente, un réseau, une base de données, le Web, des serveurs d'application, des systèmes d'exploitation, des machines virtuelles et des dispositifs de stockage de l'entrepreneur ou d'un sous-traitant.

d) Données : Toutes les données et l'information qui sont transférées, archivées, sauvegardées, stockées sur des supports ou créées dans la ***solution de SGDSL***, ou qui y sont associées, seront conservées au Canada et demeureront la propriété du GC en tout temps. Par conséquent, elles devront être chiffrées dans le respect des exigences de sécurité du GC. Les données doivent demeurer dans leur format d'origine. Ce format ne doit pas être converti en un format exclusif, car le GC doit être en mesure d'accéder à ses données en tout temps.

Voici les fonctionnalités de base visées par la portée de la ***solution de SGDSL*** :

e) **Portail pour les ressources du Bureau de la traduction** : Fournir aux professionnels du Bureau de la traduction une interface Web personnalisable fondée sur les rôles donnant accès à l'information, à l'ordonnancement, aux rapports sur les heures de travail, aux tâches ou aux activités attribuées relatives aux ***projets***, aux notes et aux états des ***projets***, aux préférences des clients du Bureau de la traduction et aux documents de référence, aux pièces jointes, à la suite d'outils du SGDSL ainsi qu'aux statistiques

personnelles, aux tableaux de bord et aux rapports en fonction du rôle de l'utilisateur, de ses droits d'accès et de ses autorisations.

f) **Portail pour les clients du Bureau de la traduction** : Fournir une interface Web personnalisable libre-service et l'accès nécessaire afin de permettre aux clients du Bureau de la traduction de présenter leurs demandes de service (***projets***) et d'en faire le suivi en temps réel tout au long du flux de travaux, et de téléverser des documents, y compris des documents de référence. Cette interface permettra également aux clients d'obtenir des devis (estimations) pour les ***projets*** et de communiquer avec les ressources du Bureau de la traduction, et donnera accès à de l'information et à des services linguistiques, y compris l'information financière et les statistiques des clients du Bureau de la traduction, les tableaux de bord et les rapports en fonction des droits d'accès et des autorisations.

g) **Portail pour les fournisseurs de services linguistiques externes** : Fournir une interface Web personnalisable et un accès à l'information et aux tâches attribuées relatives aux ***projets***, aux notes et aux états des ***projets***, aux pièces jointes ainsi qu'un accès au système de gestion des demandes du Bureau de la traduction et aux outils de traduction assistée par ordinateur, aux mémoires de traduction liées à leurs ***projets***, aux préférences et aux documents de référence des clients du Bureau de la traduction, y compris les statistiques personnelles, les tableaux de bord et les rapports en fonction des droits d'accès et des autorisations.

h) **Gestion des flux de travaux** : Fournir aux professionnels du Bureau de la traduction (personnel de soutien, équipes de projet, traducteurs, terminologues et interprètes) des outils Web personnalisables et une technologie permettant de rationaliser les processus qui permettent au Bureau de la traduction d'offrir plus efficacement à ses clients des services et des produits de qualité. Cette composante assurera l'élaboration des flux de travaux (modélisation des processus opérationnels actuels et futurs), la configuration des règles opérationnelles, la communication avec les utilisateurs tout au long du cycle de vie de la demande, la gestion des demandes (***projets***) manuelle et automatisée, le traitement des demandes (***projets***) de service des clients du Bureau de la traduction, de la réception à la livraison et à la facturation.

i) **Gestion de la charge de travail** : Fournir une interface Web personnalisable permettant la gestion des tâches et des activités, la planification, l'ordonnancement et la répartition (affectation) des ressources du Bureau de la traduction en fonction d'une échelle, d'attributs et de règles opérationnelles configurables. Cette composante permettra également la gestion des profils et des ressources humaines, ce qui peut comprendre des attributs comme le rôle, la disponibilité, les qualifications, les certifications, les langues, les habilitations de sécurité, les moyennes de mots traduits, les spécialités et les domaines de traduction (aéronautique, médical, etc.) et peut-être même la gestion de ressources matérielles comme les réservations de salles, de locaux, d'emplacements et d'équipements (audiovisuel).

j) **Gestion de la terminologie** : Fournir des bases de données terminologiques et un outil d'extraction de termes, y compris la capacité d'utiliser un produit terminologique pour traduire des termes reconnus du contenu, de documenter la terminologie spécialisée ainsi que les préférences terminologiques des clients du Bureau de la traduction, et de créer des lexiques.

k) **Outils de traduction assistée par ordinateur (TAO)** : Fournir des outils de prétraduction, d'analyses, d'édition, d'alignement, de traduction automatique et un moteur de recherche. Permettre la gestion et

l'utilisation d'une mémoire de traduction pour la traduction du contenu, la gestion, la personnalisation, la catégorisation et le regroupement du contenu en ***projet*** ou traduction de nature générale.

l) **Outils d'assurance de la qualité** : Permettre d'éditer, de réviser, de relire et de vérifier l'orthographe et la grammaire du contenu avant et après sa livraison aux clients du Bureau de la traduction et/ou sa saisie dans les outils de gestion de la terminologie ou de TAO (mémoire de traduction) afin d'assurer la qualité post-traduction.

m) **Analyses, production de rapports et vérification** : Fournir des capacités avancées d'analyse, de production de rapports et de vérification pour répondre aux besoins en matière d'information décisionnelle. Cette composante permettra également de rechercher, de filtrer et d'interroger diverses sources de métadonnées et de données pour produire des rapports personnalisés et des rapports sur les données transactionnelles, pour prendre en charge les tableaux de bord et les fiches d'évaluation (production de rapports sur les indicateurs, les normes de service opérationnelles et ministérielles et les indicateurs de rendement clés [IRC]), et pour fournir un soutien en matière de tendances et d'analyses.

n) **Interopérabilité avec les systèmes financiers** : la ***solution de SGDSL*** sera compatible avec le système financier du GC (SIGMA) afin de permettre l'échange de données pour la facturation des clients du Bureau de la traduction et la production de rapports à leur intention.

o) **Gestion de la sécurité** : Assurer l'accès à la ***solution de SGDSL***, à la suite d'outils, aux caractéristiques et fonctionnalités en fonction des profils de contrôle de sécurité en matière de TI du GC.

p) **Gestion de l'adaptabilité** : Être facilement adaptable pour permettre une augmentation et une réduction à l'échelle pour prendre en charge simultanément 2000 utilisateurs sans aucune dégradation du service.

q) **Gestion des documents** : Permettre au GC de traiter des documents jusqu'à concurrence des normes de sécurité de niveau Protégé B du gouvernement du Canada. Cette composante devrait permettre de gérer les documents tout au long du cycle de vie de la demande, de la réception à la livraison et à l'archivage final dans le dépôt. Elle devrait permettre la saisie de documents (numérisation, courriels, téléversement manuel et automatique), les recherches, l'indexation, le contrôle des versions, le traitement, la prise en charge de divers formats, la configuration de la période de conservation et l'application de contrôles et de mesures de sécurité des documents.

1.3.1 Vision et approche visant le déploiement de la *solution de SGDSL*

La ***solution de SGDSL*** offrira d'importantes possibilités de transformer et de moderniser le Bureau de la traduction. La mise en place d'un outil technologique qui normalisera, optimisera et automatisera les processus permettra au Bureau de la traduction de passer d'une approche axée sur l'exécution manuelle des demandes transactionnelles ayant peu d'utilité pour le processus à une planification stratégique des projets. Cette transformation sera facilitée par la mise en place d'outils en ligne qui permettront aux clients du Bureau de la traduction de traiter des demandes courantes exigeant des interventions limitées des employés du Bureau de la traduction. Cela permettra à ces derniers de mettre à contribution leur expertise dans le cadre d'activités plus stratégiques et complexes qui aideront le programme des services linguistiques fédéraux à produire de meilleurs résultats.

De plus, la ***solution de SGDSL*** permettra d'exécuter des activités de traduction, d'uniformisation terminologique et d'interprétation, et d'appuyer ces dernières, à l'aide d'une suite d'outils intégrés et modernes dans les

domaines de la gestion des mémoires de traduction, de la gestion de la terminologie, du contrôle de la qualité, de la planification des activités d'interprétation et de la production de rapports.

1.4 STRUCTURE DE L'ÉNONCÉ DES TRAVAUX

Le corps du présent EDT contient une description générale de la structure et du contenu de l'EDT :

	Titre	Description
Partie 1	Système de gestion des demandes de services linguistiques	Présente un résumé de la solution, le contexte, la portée, les paramètres du Bureau de la traduction, l'organisation, les services, le flux des travaux, la structure de l'EDT et La terminologie commune.
Partie 2	Exigences relatives aux lois, aux règlements et aux politiques	Fournit de l'information sur l'obligation de l'entrepreneur de se conformer aux lois, aux règlements, aux politiques, aux directives et aux normes.
Partie 3	Exigences fonctionnelles	Énumère les exigences relatives à la ***solution de SGDSL*** *et à ses composantes*.
Partie 4	Exigences techniques	Énumère les exigences techniques relatives à la ***solution*** *de SGDSL et à ses composantes*.
Partie 5	Exigences non fonctionnelles	Contient de l'information sur les engagements généraux, les exigences de sécurité, les communications, la gestion des services et l'accessibilité Web.
Partie 6	Gestion et surveillance	Fournit de l'information détaillée sur les jalons, les produits livrables et les exigences de sécurité.
Partie 7	Services professionnels	Présente une description des ressources des services professionnels de l'entrepreneur qui peuvent être nécessaires pour des travaux supplémentaires et la personnalisation de la ***solution de SGDSL***.
Partie 8 - Appendice A	Glossaire	Définit les termes utilisés dans l'EDT.
Partie 9 - Appendice B	Acronymes	Définit les acronymes et les abréviations utilisés dans l'EDT.
Partie 10 - Appendice C	Rapports du Bureau de la traduction	Fournit une liste des éventuels rapports du Bureau de la traduction.
Partie 11 - Appendice D	Responsabilités des ressources en services professionnels	Contient une liste des ressources de l'entrepreneur qui peuvent être nécessaires pour la ***solution de SGDSL***.
Partie 12 - Appendice E	Exemple et calcul de la charge de travail d'interprétation	Contient l'information utilisée pour calculer le nombre total des heures travaillées par les employés interprètes du Parlement et de conférences.
Partie 13 - Appendice F	Langues et formats de fichiers du Bureau de la traduction	Fournit une liste des langues et formats de fichiers pris en charge par le Bureau de la traduction.
Partie 14 - Appendice G	Sécurité et protection des renseignements personnels	Fournit de l'information sur les contrôles de sécurité ITSG-33, les contrôles de sécurité du SGDSL, les profils de contrôle de sécurité et la Matrice de traçabilité des exigences en matière de sécurité.

1.5 TERMINOLOGIE COMMUNE

En plus du glossaire, voici une partie comportant la définition et la signification des termes communs et récurrents du présent document.

Dans le présent EDT :

Terme	Définition
Langues officielles du Canada	Les langues officielles du Canada sont le français et l'anglais.
Fournisseur de services linguistiques (FSL)	Une ressource interne ou externe qui fournit des services linguistiques pour la traduction, la terminologie ou l'interprétation.
Solution de SGDSL	Solution commerciale complète qui fournit l'ensemble des outils et des applications d'infrastructure nécessaires, y compris les caractéristiques et les fonctionnalités prêtes à l'emploi qui permettent aux utilisateurs ainsi qu'aux ressources internes et externes d'exécuter les tâches et les activités requises pour fournir des services de traduction, de terminologie et d'interprétation aux clients du Bureau de la traduction.
Projet	Demande ou commande présentée par un client du Bureau de la traduction pour obtenir un service.
Fournisseurs	Entreprise qui peut avoir une ou plusieurs ressources pouvant fournir des services linguistiques au Bureau de la traduction.
Basé sur le Web	Permet à un utilisateur d'avoir accès à la solution et à ses applications et d'interagir avec celles-ci à l'aide d'un navigateur Web comme Internet Explorer, Chrome, Firefox ou Safari.
Les principaux termes et acronymes utilisés au fil du présent document sont définis à l'*appendice A – Glossaire* et à l'*appendice B - Acronymes*.	

1.6 BUREAU DE LA TRADUCTION

1.6.1 Aperçu

Le Bureau de la traduction gère et fournit des services de traduction, de terminologie et d'interprétation. Les tableaux suivants donnent un bref aperçu des trois secteurs d'activité du Bureau de la traduction et décrivent les services, les clients du Bureau de la traduction, ainsi que les langues (se reporter à l'*appendice F – Langues et formats de fichiers du Bureau de la traduction* pour obtenir une liste complète).

1.0 Traduction	
a) Services	I. Traduction, révision, édition et autres
b) Clients du Bureau de la traduction	I. Ministères et organismes fédéraux II. Parlement (Sénat, Chambre des communes, Librairie du Parlement et autres) III. Entreprises du secteur privé qui ont conclu un contrat avec la fonction publique fédérale.
c) Langues	I. Langues officielles du Canada II. Langues autochtones III. Langues étrangères

2.0 Terminologie	
a) Services	I. Conseils terminologiques ou linguistiques sans frais II. Glossaires bilingues ou multilingues sur mesure III. Normalisation terminologique et autres
b) Clients du Bureau de la traduction	I. Participation aux travaux de comités de terminologie II. Participation, à la demande d'un client du Bureau de la traduction, à des comités de terminologie qui ne sont pas liés au mandat de normalisation du Bureau de la traduction et qui ne concernent qu'un seul ministère ou organisme.
c) Langues	I. Langues officielles du Canada II. Langues autochtones III. Langues étrangères

3.0 Interprétation	
a) Services	I. Services d'interprétation au Parlement II. Services d'interprétation visuelle et d'interprétation de conférences.
b) Clients du Bureau de la traduction	Parlement I. Débats de la Chambre des communes II. Sénat et comités sénatoriaux III. Réunions du Cabinet et de caucus IV. Conférences de presse parlementaires V. Délibérations de la Bibliothèque du Parlement et des associations parlementaires Services d'interprétation visuelle et d'interprétation de conférences I. Sommets internationaux II. Discussions bilatérales ou multilatérales entre chefs d'État ou de gouvernement III. Conférences intra ou interministérielles IV. Rencontres entre des ministres fédéraux et leurs homologues provinciaux ou territoriaux
c) Langues	I. Langues officielles du Canada II. Langues autochtones I. Langues étrangères II. Langues visuelles (langues des signes visuels et tactiles)

1.7 DONNÉES VOLUMÉTRIQUES

En raison des limites de production de rapports des systèmes vieillissants actuellement en place, les données volumétriques du présent EDT sont fondées sur des données statistiques limitées et ne sont

fournies qu'à titre d'information.

a) Nombre de comptes actifs et inactifs des clients du Bureau de la traduction (parent) et sous-clients du Bureau de la traduction (enfant)

Code compte-client du Bureau de la traduction (XXX-XX-XX)		**Nombre de clients du Bureau de la traduction en 2017-2018**		
Structure du compte	**Exemple**	**Actifs**	**Inactifs (dans les 12 derniers mois)**	**Total**
Niveau primaire (parent) – Ministère	Services publics et Approvisionnement Canada	248	230	**478**
Niveau secondaire – Direction générale	Bureau de la traduction	1428	962	**2390**
Niveau tertiaire – Direction ou section	Réingénierie stratégique	9242	7159	**16401**

b) Volume de mots et d'activités (2016-2017)

Mots	**Volume**
Mots traduits par année	> 310 millions de mots

Activités		**Quantité**
Activités d'interprétation parlementaire	Langues officielles et autochtones (sur demande)	~ 5040
Activités d'interprétation pour des conférences	Langues officielles et autochtones	1801
	Langues étrangères	382
Activités d'interprétation visuelle	Langue des signes québécoise (LSQ), American Sign Language (ASL), Interprétation orale en français et en anglais (lecture labiale), Interprétation tactile pour personnes sourdes et aveugles	1577

c) Nombre de fournisseurs de services linguistiques (FSL) en traduction et interprétation (2016-2017)

Fournisseurs de services linguistiques (FSL)		**Nombre**
Traducteur interne	Langues officielles et étrangères	895

Fournisseurs de services linguistiques (FSL)			Nombre
Interprétation interne	Parlementaire	Langues officielles	39
	Conférence	Langues officielles et étrangères	25
Interprétation externe (FSL)	Parlementaire	Langues officielles	30
		Langues étrangères et autochtones	~ 10 à 15
	Conférence	Langues étrangères et autochtones	145
		Langues étrangères	160
	Visuelle	Langue des signes québécoise (LSQ) American Sign Language (ASL) Interprétation orale en français et en anglais (lecture labiale) Interprétation tactile pour personnes sourdes et aveugles	~ 150

d) Le Bureau de la traduction utilise de nombreuses bases de données, et deux d'entre elles sont d'une grande importance pour les activités au quotidien. La première est le « bio-corpus », un dépôt pour les documents en langue de départ complets formatés et les documents en langue d'arrivée finaux formatés. Le second est le « méga-corpus », le dépôt de la mémoire de traduction pour tous les segments de traduction appariés et alignés utilisés par les ressources du Bureau de la traduction.

Le tableau suivant montre la capacité de base, la capacité utilisée, la capacité restante et le changement en pourcentage d'année en année.

Nom de la base de données	Capacité	Utilisée	Restante	Changement en pourcentage d'année en année
Bio-corpus	1,0 To	968 Go	32 Go	~ 16 %
Méga-corpus	481 Go	279 Go	175 Go	~ 16 %
To = Téraoctet, Go = Gigaoctet				

1.8 SECTEURS, FONCTIONS OPÉRATIONNELLES ET ACTIVITÉS CLÉS DU BUREAU DE LA TRADUCTION

Le Bureau de la traduction compte plusieurs secteurs : Centre de contact (CC); Centre de traitement des demandes (CTD); Centre de traduction et de terminologie (CTT); Centre d'appui professionnel (CAP); Service au Parlement, interprétation de conférences et interprétation visuelle. Le Bureau de la traduction gère des services de traduction, de terminologie et d'interprétation qu'il fournit à ses clients, et chacun de ses secteurs exerce des fonctions et des activités opérationnelles de base différentes.

Le tableau suivant contient une liste des secteurs du Bureau de la traduction et de leurs fonctions opérationnelles et activités clés.

1.0 Centre de contact (CC)		
1.1	**Fonction opérationnelle**	a) Recevoir et traiter les demandes d'information et de service des clients du Bureau de la traduction, des ***fournisseurs,*** des employés et du grand public.
1.2	**Activités clés**	a) Recevoir tous les appels téléphoniques et courriels transmis aux points de contact généraux du Bureau de la traduction par des clients du Bureau de la traduction, des ***fournisseurs***, des employés et des membres du grand public. b) Traiter et fermer les demandes générales selon les normes de service établies. c) Acheminer les demandes complexes aux centres d'expertise pertinents.

2.0 Centre de traitement des demandes (CTD)		
2.1	**Fonction opérationnelle**	a) Évaluer la charge de travail en matière de services linguistiques et l'attribuer aux ressources internes et aux ***fournisseurs*** et faire un suivi des progrès.
2.2	**Activités clés**	a) Évaluer les demandes de service soumises par les clients du Bureau de la traduction. b) Établir et coordonner les estimations. c) Planifier et coordonner les travaux. ***d)*** Attribuer la charge de travail aux ressources internes et aux ***fournisseurs***. e) Surveiller l'état d'avancement du traitement des demandes, de la réception jusqu'à la livraison. f) Évaluer la capacité contractuelle externe.

3.0 Centre de traduction et de terminologie (CTT)		
3.1	**Fonctions opérationnelles**	a) Fournir des produits et des services de traduction et de terminologie au Parlement, à l'appareil judiciaire et aux ministères et organismes fédéraux dans les deux langues officielles, en langue visuelle ainsi que dans d'autres langues. b) Fournir ces services, sur demande, à d'autres administrations publiques du Canada et à des organismes internationaux. c) Normaliser la terminologie utilisée au gouvernement fédéral.
3.2	**Activités clés**	a) Fournir des services de traduction et de révision des textes traduits à l'interne et par des ***fournisseurs***. b) Évaluer le travail des ***fournisseurs***. c) Normaliser la terminologie. d) Produire des bulletins de terminologie, des lexiques et des vocabulaires. e) Gérer les bases de données terminologiques du Bureau de la traduction. f) Assurer la qualité.

4.0 Centre d'appui professionnel (CAP)		
4.1	**Fonction opérationnelle**	a) Offrir des services d'appui professionnel aux langagiers internes, aux ***fournisseurs*** et aux clients du Bureau de la traduction.
4.2	**Activités clés**	a) Prendre en charge les demandes de recherches terminologiques et documentaires des ressources internes et des ***fournisseurs***. b) Gérer et tenir à jour le fonds documentaire et les trousses de référence à l'intention des traducteurs du Bureau de la traduction et des ***fournisseurs***. c) Faire une relecture des fiches terminologiques avant diffusion. d) Exécuter l'extraction automatique et le dépouillement terminologique, et rédiger des fiches provisoires. e) Formater les documents pour assurer une présentation conforme. f) Fournir des services de transcription aux clients du Bureau de la traduction et aux membres de l'organisation. g) Effectuer la correction d'épreuves des documents avant la livraison. h) Traiter les documents de travail provenant du Centre de traitement des demandes. i) Gérer le contenu des mémoires de traduction. j) Livrer les documents.

5.0 Service au Parlement, interprétation de conférences et interprétation visuelle		
5.1	**Fonctions opérationnelles**	a) Offrir des services d'interprétation au Parlement, à l'appareil judiciaire et aux ministères et organismes fédéraux dans les deux langues officielles, en langue visuelle ainsi que dans d'autres langues. b) Fournir ces services, sur demande, à d'autres administrations publiques du Canada et à des organismes internationaux. c) Accréditer les interprètes.
5.2	**Activités clés**	a) Fournir des services d'interprétation en faisant appel à des interprètes internes et des ***fournisseurs*** (FSL). b) Évaluer le travail des ***fournisseurs***.

Les ressources au sein de chaque secteur peuvent se voir attribuer un ou plusieurs rôles, selon la nature du travail requis pour remplir la fonction opérationnelle de base. Ces rôles sont généralement associés à des tâches et des activités; une fois attribués, ils peuvent fournir les droits d'accès et les autorisations aux caractéristiques et fonctionnalités des outils nécessaires à l'accomplissement des tâches et des activités.

1.9 SERVICES DU BUREAU DE LA TRADUCTION

Voici une liste des services offerts actuellement par le Bureau de la traduction.

Service	Description
Adaptation	Traduire un document en apportant des changements pour adapter le message selon le public cible.

Service	Description
Services administratifs	Traiter une demande nécessitant un niveau de traitement administratif inhabituel. Par exemple, le traitement de demandes comportant plusieurs fichiers, de fichiers complexes et/ou de fichiers qui exigent un traitement particulier (comme les fichiers PDF et JPG), la fusion de fichiers et la recherche de documents qui ont déjà été traduits.
Service d'urgence après les heures	Fournir des services de traduction ou des services linguistiques en dehors des heures normales de bureau, le weekend ou les jours fériés.
Interprétation de conférences	Fournir des services d'interprétation de conférences en langues officielles, autochtones, étrangères et visuelles/gestuelles.
Révision comparative	Effectuer une comparaison rigoureuse d'une traduction avec le texte original, et, s'il y a lieu, corriger le contenu et le style de la traduction.
Révision d'une rédaction (unilingue)	Améliorer un texte original en apportant des corrections grammaticales ou stylistiques ou en proposant des solutions pour qu'il soit plus facile à lire et à comprendre.
Révision d'une rédaction (unilingue) et traduction	Réviser un document original, puis le traduire.
Révision d'une rédaction (unilingue) et traduction d'un document bilingue	Réviser un document comportant du texte dans deux langues, puis le traduire de façon à en faire un document complet dans les deux langues.
Révision d'une rédaction (unilingue), traduction et révision comparative	Réviser un document original, puis le traduire et, finalement, effectuer une comparaison détaillée du texte original avec sa traduction afin de corriger, s'il y a lieu, le contenu et le style de cette dernière.
Traducteur sur place	Fournir les services d'un langagier qui peut travailler exclusivement et de façon autonome chez un client ou un groupe de clients du Bureau de la traduction, dans leurs locaux ou, dans des circonstances exceptionnelles, dans les locaux du Bureau de la traduction.
Interprétation parlementaire	Fournir des services d'interprétation en langues officielles au Parlement.
Évaluation professionnelle	Évaluer en détail la qualité de traductions, de révisions ou de tout texte rédigé en français ou en anglais, selon des critères reconnus d'équité et d'objectivité. L'évaluation est présentée sous forme d'un rapport détaillé (avec exemples à l'appui) ou de commentaires concis sur chaque texte.
Gestion de projet	Planifier, organiser, diriger, contrôler et surveiller un ***projet*** linguistique ou de traduction complexe.
Correction d'épreuves	Lire les épreuves, repérer les fautes et les coquilles, et indiquer, s'il y a lieu, les changements à apporter.
Révision d'un document bilingue	Réviser un document comportant du texte dans deux langues.

Service	Description
Traduction à vue	Traduire un document verbalement, en personne ou par téléphone.
Résumé	Fournir un résumé écrit ou verbal d'un document dans la même langue ou dans une autre langue.
Services de terminologie	Créer des glossaires personnalisés, participer au nom des clients du Bureau de la traduction à des comités sur la terminologie et exécuter d'autres ***projets*** terminologiques.
Traduction	Transposer un texte dans une langue en tenant compte du ton, du style et de la terminologie utilisés par l'auteur.
Traduction et révision comparative	Traduire un document puis faire réviser la traduction par un autre professionnel. Recommandé pour les documents destinés à un public de prestige ou au grand public et pour les documents à grande diffusion ou de grande incidence.
Traduction d'un document bilingue	Traduire un document qui contient du texte dans deux langues.
Traduction de modifications	Traduire des modifications apportées à un texte déjà traduit.
Traducteur en attente	Fournir les services d'un langagier professionnel qui peut, moyennant un préavis minimal, être joint en tout temps pendant une période déterminée pour effectuer du travail pour un client du Bureau de la traduction. Le traducteur peut, toutefois, exécuter d'autres tâches pendant ce temps.
Aide à la rédaction	Rédiger un texte en collaboration avec un client du Bureau de la traduction et formuler des conseils linguistiques sur des problèmes de traduction et des questions de langue (grammaire, style, ponctuation, terminologie, etc.).

1.10 FLUX DE TRAVAUX DU BUREAU DE LA TRADUCTION

1.10.1 Aperçu

Le Bureau dispose de certains flux de travaux pour fournir des services de traduction, de terminologie et d'interprétation aux clients du Bureau de la traduction. Les flux de travaux regroupent plusieurs secteurs comportant diverses tâches et activités axées sur les services demandés.

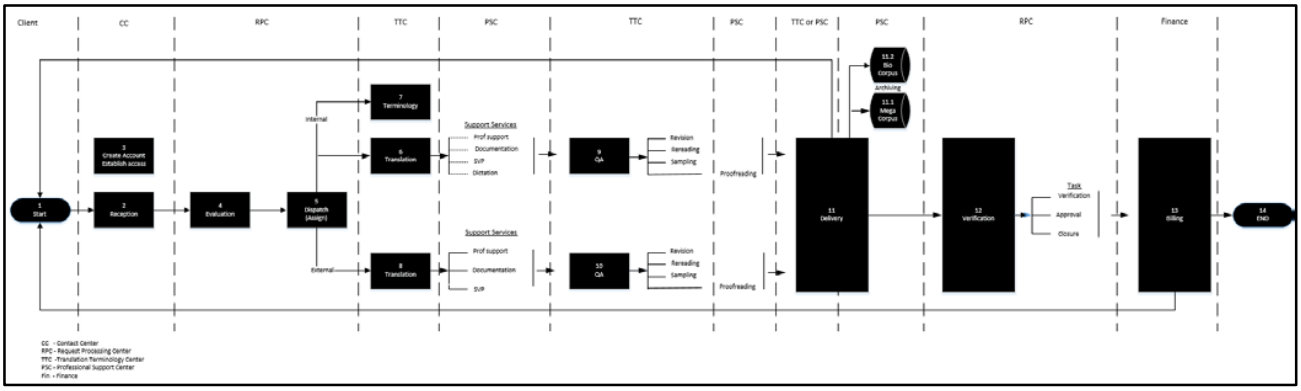
En ce qui a trait à la ***solution de SGDSL***, la gestion du flux de travaux est une composante essentielle et est étroitement liée aux exigences fonctionnelles du présent EDT, par exemple la gestion de la charge de travail, les portails pour les clients et les ressources du Bureau de la traduction, les profils clients du Bureau de la traduction et ceux des ressources, les analyses, les rapports et l'information décisionnelle. Les caractéristiques et les fonctionnalités de la composante de gestion du flux des travaux, de concert avec les autres exigences, permettraient au Bureau de la traduction de réduire les interventions manuelles ainsi que d'automatiser et de

gérer de manière plus efficace et efficiente les services, les demandes des clients du Bureau de la traduction, les ressources internes et externes, la charge de travail, les tâches et les activités afin d'offrir des services de qualité.

Pour donner un exemple des tâches et des activités en cours au sein du Bureau de la traduction, un résumé général d'un flux de travaux de traduction est présenté ci-dessous. Il est important de noter qu'au moment de la rédaction du présent document, les autres flux de travaux relatifs à la terminologie et à l'interprétation (parlementaire, conférence et visuelle) n'étaient pas terminés et facilement accessibles. Une fois terminés, ils pourront être fournis sur demande.

1.10.2 Flux de travaux de traduction

Voici un flux de travaux de traduction général, de la soumission d'une demande de service par un client du Bureau de la traduction jusqu'à la livraison du texte à celui-ci.



1.10.2.1 Information détaillée sur le flux de travaux de traduction général

Le tableau ci-dessous présente de façon générale les tâches, les activités et les intervenants actuels ainsi qu'une description du flux de travaux de traduction.

Nombre	Intervenant	Tâche/activité	Description
1	Client du Bureau de la traduction	Début	Le client du Bureau de la traduction soumet sa demande par l'entremise du système du Bureau de la traduction. La demande peut également être soumise par courriel ou par d'autres moyens si le client du Bureau n'a pas accès au système ou si la sécurité des documents ne lui permet pas de joindre la demande.
2	CC	Réception	Le Bureau de la traduction reçoit la demande de son client par l'entremise de son système, par courriel ou par d'autres moyens. Il télécharge les documents à traduire et les documents de référence. Il analyse ces documents pour obtenir le nombre de mots et les compare avec le contenu de la mémoire de traduction.
3	CC	Création d'un compte Établissement de l'accès	Deux types de compte doivent être créés pour utiliser le système : 1. Le compte du client du Bureau de la traduction doit être créé au préalable. Les

Nombre	Intervenant	Tâche/activité	Description
			informations de facturation doivent être saisies au niveau du compte-client. 2. Le client du Bureau doit avoir un compte-utilisateur. Les comptes-utilisateurs sont uniques et sont liés au compte-client. Plusieurs utilisateurs peuvent être associés à un même compte-client.
4	CTD	Évaluation	Le Bureau de la traduction analyse la demande du client et valide le service demandé et la date d'échéance. Après avoir consulté le client, le conseiller modifie la demande si nécessaire.
5	CTD	Répartition (attribution)	La demande est attribuée en fonction du domaine, de sa langue et du temps alloué. La demande est répartie en fonction du domaine, de la langue et du temps requis et est divisée en tranches si elle est trop importante pour qu'un seul traducteur puisse respecter l'échéance.
6	CTT	Traduction	Un traducteur du Bureau de la traduction traduit le document.
6	CAP	Services d'appui	Le Centre d'appui professionnel offre plusieurs services qui permettent aux traducteurs de se consacrer à la traduction, y compris les suivants : soutien professionnel (chiffrement, conversion de documents et autres), services documentaires, édition et transcription.
7	CTT	Terminologie	Les traducteurs ont accès à des trousses terminologiques propres aux clients afin d'assurer la cohérence du vocabulaire, des acronymes et d'autres informations pertinentes pour les clients. Les trousses terminologiques sont tenues à jour par des spécialistes du contenu du Bureau de la traduction.
8	CTT	Traduction	Un fournisseur de services linguistiques externe traduit le document.
8	CAP	Services d'appui	Le Centre d'appui professionnel offre plusieurs services aux fournisseurs de services linguistiques externes afin de leur permettre de respecter certaines normes et de normaliser la traduction du client du Bureau de la traduction, y compris les suivants : soutien professionnel (chiffrement, conversion de documents et autres), services documentaires, éditique.
9	CTT	Assurance de la qualité	Un texte traduit à l'interne est révisé ou relu en fonction de la nature du document. Il peut également faire l'objet d'une correction d'épreuves si le traducteur le souhaite et si le temps le permet.
10	CTT	Assurance de la qualité	Les traductions fournies par un fournisseur de services linguistiques externe sont révisées ou relues en fonction de la nature du document. Si la nature du document

Nombre	Intervenant	Tâche/activité	Description
			n'exige pas de révision ou de relecture, il doit passer par le processus d'échantillonnage avant d'être soumis à une correction d'épreuves puis livré au client du Bureau de la traduction.
11	CTT ou CAP	Livraison	Livraison des documents traduits au client du Bureau de la traduction.
11.1	CAP	Archivage – Méga-corpus	Le méga-corpus contient des documents d'archives (documents sources et documents traduits) segmentés et indexés pour utilisation par les moteurs de recherche du Bureau de la traduction.
11.2	CAP	Archivage – Bio-corpus	Le bio-corpus contient tous les documents d'archives (documents sources et documents traduits) du Bureau de la traduction dans leur format original. Le bio-corpus est utilisé pour alimenter le méga-corpus.
12	CTD	Vérification	Vérification des tâches et des unités à facturer dans le cadre du processus de facturation.
13	Finances	Facturation	Ce processus est exécuté deux fois par mois selon un calendrier établi. Le système du Bureau de la traduction calcule le montant des factures et génère un message qui est envoyé à SIGMA (SAP). Une fois les données traitées dans SIGMA, il produit un fichier qui est téléversé dans le système du Bureau de la traduction afin de faire concorder les données de facturation de SIGMA avec celles du système du Bureau de la traduction.
14	FIN	FIN	La demande a été traitée, livrée et facturée.

2 EXIGENCES RELATIVES AUX LOIS, AUX RÈGLEMENTS ET AUX POLITIQUES

2.1 INTRODUCTION

La ***solution du SGDSL*** doit permettre au GC de se conformer à l'ensemble de ses lois, règlements, politiques, directives, normes et lignes directrices, tel que détaillé ci-dessous. La ***solution du SGDSL*** doit être conforme à l'ensemble des lois, des règlements, des politiques, des directives, des normes et des lignes directrices.

Veiller à la sécurité et à la protection des renseignements personnels demeure une priorité pour SPAC. La ***solution du SGDSL*** et l'entrepreneur doivent se conformer à l'ensemble des lois applicables y compris, sans toutefois s'y limiter, celles qui se rapportent au respect de la vie privée ainsi qu'au traitement et au stockage de renseignements personnels.

2.2 LOIS, REGLEMENTS, POLITIQUES, DIRECTIVES, NORMES ET LIGNES DIRECTRICES

L'entrepreneur et la ***solution du SGDSL*** doivent se conformer aux lois, aux règlements, aux politiques, aux directives, aux normes, aux lignes directrices et aux spécifications suivants du GC, sans toutefois s'y limiter :

Type	Titre	Adresse URL
Politiques	Politique sur la protection de la vie privée	https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510
	Politique sur la sécurité du gouvernement	https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578
	Mise en œuvre de HTTPS pour les connexions Web sécurisées : Avis de mise en œuvre de la Politique sur la technologie de l'information (AMPTI)	https://www.canada.ca/fr/secretariat-conseil-tresor/services/technologie-information/avis-mise-oeuvre-politique/mise-oeuvre-https-connexions-web-securisees-ampti.html
	Orientation relative à la résidence des données électroniques	https://www.canada.ca/fr/secretariat-conseil-tresor/services/technologie-information/avis-mise-oeuvre-politique/orientation-relative-residence-donnees-electroniques.html
Lois	*Loi sur les langues officielles*	http://laws-lois.justice.gc.ca/fra/lois/O-3.01/index.html
	Loi sur la protection des renseignements personnels	http://laws-lois.justice.gc.ca/fra/lois/p-21/
	Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)	http://laws-lois.justice.gc.ca/fra/lois/P-8.6/index.html
	Norme sur la gestion de la sécurité des technologies de l'information (GSTI)	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12328
Lignes directrices	ITSG-22 Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada	https://www.cse-cst.gc.ca/fr/node/268/html/28461

Type	Titre	Adresse URL
	ITSG-33 La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (en conformité avec le PCS)	https://www.cse-cst.gc.ca/fr/publication/itsg-33
	ITSG-38 Établissement des zones de sécurité dans un réseau — Considérations de conception relatives au positionnement des services dans les zones	https://www.cse-cst.gc.ca/fr/node/266/html/27445
	ITSP.40.111 Algorithmes cryptographiques pour l'information NON CLASSIFIÉE, PROTÉGÉ A et PROTÉGÉ B	https://www.cse-cst.gc.ca/fr/publication/list/Cryptography
	ITSP.30.031 V3 Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information	https://www.cse-cst.gc.ca/fr/node/2454/html/28582
	AMPTI : 2014-01 Questions de sécurité relatives à l'utilisation de supports amovibles pour les renseignements Protégé C et classifiés	https://www.cse-cst.gc.ca/fr/node/1224/html/2269
	GRC G1-001 Guide d'équipement de sécurité	http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_f.htm
Normes	WCAG2.0 Accessibility (Accessibilité)	http://www.w3.org/TR/WCAG20/
Spécifications	CVSS v3.0 Common Vulnerability Scoring System v3.0 (Système commun d'évaluation des vulnérabilités)	https://www.first.org/cvss/specification-document

Toutes les lois fédérales, y compris celles qui ne sont pas énumérées ci-dessus, peuvent être consultées dans leur intégralité sur le site Web du ministère de la Justice : www.justice.gc.ca.

3 EXIGENCES FONCTIONNELLES

3.1 INTRODUCTION AUX EXIGENCES FONCTIONNELLES

Les exigences fonctionnelles précisent la portée des travaux, notamment les activités précises qui doivent être réalisées par l'entrepreneur, ainsi que les capacités globales que doit comprendre la ***solution du SGDSL*** tout en étant conforme aux exigences obligatoires des lois et des politiques applicables, propres à chaque sous-activité. L'entrepreneur doit exécuter les activités suivantes et fournir une ***solution du SGDSL*** qui comprend :

a) Un outil interactif sur le Web personnalisable et facilement configurable par les utilisateurs en fonction de leurs besoins particuliers.
b) La possibilité de définir les permissions, les droits d'accès et les rôles d'utilisateurs pour la solution, la suite d'outils, les fonctionnalités et les caractéristiques.
c) Des règles administratives et de flux de travaux qui seront configurées par les utilisateurs pour faciliter une grande variété de processus, d'activités et de fonctions.
d) La possibilité de gérer efficacement les données et les métadonnées. Autrement dit, toutes les données seront saisies une seule fois et validées dans la Solution. Elles pourront être réutilisées et mises à profit dans l'ensemble de la Solution ainsi que d'une fonctionnalité à l'autre.
e) La possibilité d'échanger sur une base continue des données dans la Solution et avec les autres systèmes connexes hébergés par l'entrepreneur.
f) Le soutien de la réutilisation des données couramment requises, et ce, de façon sécurisée à l'échelle de la Solution et dans d'autres systèmes de SPAC.
g) La possibilité d'apporter des changements constants et d'accéder en temps réel aux données, aux rapports et à l'information analytique pour appuyer la gestion efficace et la prise de décisions opérationnelles de SPAC, la surveillance et le suivi des processus et du rendement.

L'entrepreneur doit intégrer complètement toutes les exigences fonctionnelles à moins d'avis contraire, comme il est décrit aux sections A à I de la *partie 3, Exigences fonctionnelles* de l'EDT.

3.2 SECTION A – EXIGENCES GÉNÉRALES

3.2.1 Objectif

La section sur les exigences générales présente les fonctions et les résultats de portée générale qui sont applicables à l'ensemble des éléments de la ***solution du SGDSL***.

3.2.2 Exigences

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
GEN-SOLN-01	**Solution** La ***solution du SGDSL*** doit être un logiciel-service géré par l'entrepreneur, qui sera hébergé par l'entrepreneur ou un par un sous-traitant, qui est sécurisé, fonctionne, est complet, sans bogue et est entièrement hébergé au Canada, ce qui comprend les centres de données de l'entrepreneur ou de sous-traitants, l'infrastructure de service sous-jacente, le réseau, la base de données, le Web, les serveurs d'application, les systèmes d'exploitation, les machines virtuelles et le stockage.

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
GEN-DATA-02	**Données et renseignements** Toutes les données et tous les renseignements qui sont transférés, archivés, sauvegardés, stockés sur des supports, créés ou associés à la ***solution du SGDSL*** doivent résider au Canada et demeureront la propriété du Canada en tout temps et, à ce titre, devront être chiffrés en fonction des exigences de sécurité du GC (« le gouvernement du Canada », « le GC » ou « le Canada »). Les données doivent demeurer dans le format d'origine et ne doivent pas être converties en format exclusif, car le Canada doit pouvoir accéder à ses données en tout temps.
GEN-WEB-03	***Basé sur le Web*** Les caractéristiques et les fonctionnalités complètes de la ***solution du SGDSL*** pour la traduction, la terminologie et l'interprétation doivent être basées sur le ***Web*** et inclure des portails (client, ressources internes et externes), des tableaux de bord, les flux de travaux, la charge de travail, la terminologie, la gestion de la sécurité, les outils de traduction assistée par ordinateur (TAO), les mémoires de traduction, la base de données terminologiques, les analyses, les rapports et les renseignements d'affaires.
GEN-SIGMA-04	**Interopérabilité avec SIGMA (SAP)** : La ***solution du SGDSL*** doit comporter les fonctionnalités suivantes en vue : a) d'assurer le transfert de tous les renseignements financiers pertinents entre la ***solution du SGDSL*** et SIGMA, au moyen des fonctionnalités d'importation et d'exportation de fichiers à destination et en provenance d'une plateforme d'atterrissage. b) d'assurer la vérification des renseignements contractuels du fournisseur au moyen de SIGMA.
GEN-IMPEXP-05	**Importation et exportation** La ***solution du SGDSL*** doit comporter les fonctionnalités suivantes : a) importer des données, des fichiers, des rapports, des analyses, des résultats d'interrogation dans la ***solution du SGDSL*** sous différents formats, dont MS Word (doc, docx), MS Excel (xls, xlsx), txt, pdf, xml, tmx, tbx et csv. b) exporter des données, des fichiers, des rapports, des analyses, des résultats d'interrogation de la ***solution du SGDSL*** sous différents formats, dont MS Word (doc, docx), MS Excel (xls, xlsx), txt, pdf, xml, tmx, tbx et csv. Nota : Pour une liste des formats de fichiers utilisés par le Bureau de la traduction, voir l'*Appendice F – Langues et formats de fichiers du Bureau de la traduction.*
GEN-SFTP-06	**Protocole sécurisé de transfert des fichiers (PSTF)** La ***solution du SGDSL*** doit prendre en charge le protocole sécurisé de transfert des fichiers.

SECTION DE L'EDT	Exigence (COTÉE)
GEN-SRCH-07	**Recherche** La ***solution du SGDSL*** devrait fournir la fonctionnalité de recherche basée sur les champs à déclarer, les attributs de document et les métadonnées.

SECTION DE L'EDT	Exigence (COTÉE)
GEN-USAB-08	**Convivialité** La ***solution du SGDSL*** devrait fournir les fonctionnalités permettant à un utilisateur ayant le rôle, les droits d'accès et les permissions nécessaires d'adapter et de configurer l'interface utilisateur et les attributs, de contrôler le comportement opérationnel (comme les conditions qui doivent être remplies avant que l'utilisateur puisse modifier une demande de service) en utilisant les règles opérationnelles et la validation des entrées.
Interface utilisateur La ***solution du SGDSL*** doit comporter les fonctionnalités suivantes :	
GEN-INTFC-09.1	Configurer l'interface-utilisateur comme suit : a) ajouter de nouvelles caractéristiques ou modifier la fonctionnalité des caractéristiques existantes; b) établir les types de caractéristiques, comme les nombres, le texte libre, les listes de sélection ou les valeurs booléennes; c) configurer l'onglet de commandes et la position de l'interface graphique utilisateur de la caractéristique; d) configurer les propriétés et le comportement à l'échelle de la caractéristique (étiquettes, aide au moyen du pointage de la souris, obligatoire/facultatif, visibilité, valeur par défaut, etc.); e) créer des règles opérationnelles et des règles de validation des valeurs entrées; f) établir la mise en page des impressions; g) préciser les caractéristiques de données déjà inscrites au moment de la création de l'élément (comme les données de l'utilisateur à partir de son profil au moment de la création de la demande); h) préciser le comportement (règles opérationnelles, règles de validation, etc.) qui s'applique au moment de la modification du processus opérationnel; i) suivre et être capable d'afficher les changements (historique) pour chaque entrée et transaction opérationnelle; j) modifier l'information, l'approbation ou le refus du flux de travaux et les soumissions à des ressources externes, et confirmer; k) configurer la disposition de l'interface utilisateur d'un portail; l) indiquer et soumettre à l'entrepreneur les changements aux valeurs, aux attributs et aux champs de données incorporés au système dans l'interface utilisateur.
GEN-INTFC-09.2	L'interface des composantes de la ***solution du SGDSL*** devrait fournir de brèves instructions d'utilisation et des conseils d'une manière uniforme pour toutes les commandes et tous les affichages.
GEN-INTFC-09.3	L'interface des composantes de la ***solution du SGDSL*** devrait suivre une norme, un thème et un ton de texte dans l'ensemble de la composante.
GEN-INTFC-09.4	La ***solution du SGDSL*** devrait prendre en charge la sélection de couleurs personnalisable et d'autres options de configuration visuelle pour permettre à SPAC de rendre l'interface conformément aux normes.
Aide en ligne La ***Solution du SGDSL*** devrait comporter les fonctionnalités suivantes :	

SECTION DE L'EDT	Exigence (COTÉE)
GEN-HELP-10.1	Une section de référence configurable contenant les liens vers des guides de référence rapides, des manuels, des tutoriels et des politiques.
GEN-HELP-10.2	De l'aide et du soutien intégrés concernant les caractéristiques, les fonctionnalités et les processus.
GEN-HELP-10.3	La présentation de sujets d'aide contextuelle correspondant à la section de la ***solution du SGDSL*** avec laquelle travaille l'utilisateur.
GEN-HELP-10.4	La ***solution du SGDSL*** devrait avoir une une fonction de foire aux questions accessible en tout temps pendant l'utilisation, sans perdre le contexte de la transaction en cours, et qui permet une navigation par sujet.
GEN-ERR-11	**Messages d'erreur, alertes et avis** La ***solution du SGDSL*** devrait permettre à un utilisateur ayant les permissions, les droits d'accès et les rôles appropriés de configurer et de contrôler les messages d'erreur, les alertes et les notifications du système ainsi que leurs déclencheurs.
GEN-DOC-12	**Documentation** L'entrepreneur devrait fournir à SPAC toute la documentation et tous les matériaux collatéraux disponibles pour la solution actuelle et toutes les versions futures.
Mises en page Web, modèles et configuration des formulaires La ***solution du SGDSL*** devrait fournir à l'utilisateur avec les permissions, les droits d'accès et les rôles appropriés de :	
GEN-CONFIG-13.1	Créer et configurer la mise en page Web, les modèles et les formulaires;
GEN-CONFIG-13.2	être en mesure de faire ce qui suit à la mise en page Web, aux modèles et aux formulaires a) configurer les champs obligatoires ou facultatifs, b) configurer et établir des valeurs par défaut pour les champs de saisie de données courants, c) ajouter des champs définis par les utilisateurs à tout écran ou onglet, d) gérer des éléments de données existants et définir de nouveaux éléments de données comprenant diverses caractéristiques, comme des règles opérationnelles, des règles de validation prédéfinies, des plages de valeurs, des listes déroulantes, des textes non imposés, selon les longueurs maximales définies par l'utilisateur, e) configurer et créer différents types de zones intrinsèques, f) commandes d'entrée : cases à cocher, boutons radio, listes déroulantes, boîtes de listes, boutons, champs de texte, champs de date, fenêtres de terminal textuelles, g) composantes de navigation : pistes de navigation, barres de défilement, champs de recherche, pagination, balises, icônes, onglets, h) composantes informationnelles : infobulles, icônes, barres de progression, notifications, boîtes ou fenêtres de message, boîtes de dialogue, fenêtres modales (fenêtres contextuelles), i) menus : barres de menu, menus, menus contextuels, menus supplémentaires, menus primaires et secondaires, j) modifier les étiquettes de champs en dehors des cases, k) notifier automatiquement les utilisateurs lorsque des champs de données obligatoires sont incomplets,

SECTION DE L'EDT	Exigence (COTÉE)
	l) modifier les indicateurs de rendement clés (IRC) ainsi que les normes de service opérationnelles et ministérielles qui peuvent changer d'année en année.
GEN-PRJCT-14	**Projets (demandes)** La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes a) empêcher les clients de soumettre des demandes de traduction incomplètes et fournir de l'information sur les mesures correctives; b) changer l'état d'une demande si l'utilisateur a les permissions, les droits d'accès et les rôles appropriés; c) annuler une demande et envoyer une notification au client si l'utilisateur a les permissions, les droits d'accès et les rôles appropriés; d) créer manuellement et automatiquement un devis et le transmettre au client si l'utilisateur détient les permissions, les droits d'accès et les rôles appropriés.
GEN-ACCS-15	**Limiter l'accès** La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de restreindre l'accès aux caractéristiques et aux fonctionnalités.
GEN-WCAG-16	**Accessibilité Web** Les pages Web de la ***solution du SGDSL*** devraient être conformes au niveau AA de la norme WCAG 2.0.

3.3 SECTION B – EXIGENCES LINGUISTIQUES

Comme l'exige la *Loi sur les langues officielles*, SPAC est tenu de donner les services dans les langues officielles du Canada.

L'entrepreneur doit rendre disponibles toutes les composantes destinées aux utilisateurs contenues dans les applications, les services, les renseignements et les outils de la ***solution du SGDSL*** (comme le texte en arrière-plan, les applications Web, les messages d'erreur ou d'avertissement, les tableaux du système, les messages générés par le système et tout document imprimé ou en ligne) sont disponibles dans les deux langues officielles du Canada.

L'entrepreneur doit :

a) fournir les documents à l'intention des utilisateurs dans les deux langues officielles, y compris le matériel de formation;
b) communiquer avec les utilisateurs dans la langue de leur choix, l'anglais étant la langue par défaut si l'utilisateur n'a pas indiqué de préférence;
c) consigner la préférence linguistique de l'utilisateur, de sorte que toutes les communications personnelles sont adressées dans la langue de son choix.
d) veiller à ce que tous les documents de communication axés sur l'utilisateur soient distribués dans les deux langues officielles du Canada;
e) veiller à ce que la ***solution du SGDSL*** et la suite d'outils soient disponibles dans la langue officielle choisie par l'utilisateur.

3.3.1 Objectif

La ***solution du SGDSL*** doit satisfaire aux obligations relatives aux langues officielles du GC, en verte de la *Loi sur les langues officielles* (http://laws-lois.justice.gc.ca/fra/lois/O-3.01/index.html).

3.3.2 Exigences

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
LANG-01	L'ensemble de la ***solution du SGDSL*** doit être disponible dans les deux langues officielles du Canada et comprendre les éléments suivants : interface utilisateur Web et d'application, système, outils, documentation, formation et bureau de service.
LANG-02	Les outils et les applications de la ***solution du SGDSL*** devraient permettre à tous les utilisateurs de définir une langue par défaut pour leur utilisation, si l'utilisateur n'a pas indiqué de préférence.

SECTION DE L'EDT	Exigence (COTÉE)
LANG-03	Devrait prendre en charge l'anglais canadien et le français canadien.
LANG-04	Les éléments d'interface utilisateur de la ***solution du SGDSL*** suivants devraient être disponibles dans les deux langues officielles du Canada : a) commandes d'entrée : cases à cocher, boutons radio, listes déroulantes, boîtes de listes, boutons, champs de texte, champs de date, fenêtres de terminal textuelles; b) composantes de navigation : pistes de navigation, barres de défilement, champs de recherche, pagination, balises, icônes, onglets; c) composantes informationnelles : infobulles, icônes, barres de progression, notifications, boîtes ou fenêtres de message, boîtes de dialogue, fenêtres modales (fenêtres contextuelles); d) menus : barres de menu, menus, menus contextuels, menus supplémentaires, menus primaires et secondaires; ~~e)~~ navigateur : Microsoft Internet Explorer 11, Edge (et deux versions antérieures); f) page de renvois, page d'accueil, page de bienvenue ou page d'ouverture de session.
LANG-05	Lors de l'utilisation des outils et des applications de la ***solution du SGDSL***, l'utilisateur devrait être en mesure de passer d'une langue officielle du Canada à l'autre.
LANG-06	Les applications et outils de la ***solution du SGDSL***, devraient permettre que certains champs de contrôle de saisie soient entrés dans les deux langues officielles du Canada, peu importe la langue qu'a choisie l'utilisateur.
LANG-07	Les outils et les applications de la ***solution du SGDSL***, devraient être capables d'intégrer l'information dans les deux langues officielles du Canada dans sa ou ses bases de données.
LANG-08	Les rapports générés dans la ***solution du SGDSL***, par les utilisateurs et les ressources devraient être disponibles dans les deux **l**angues officielles du Canada.

SECTION DE L'EDT	Exigence (COTÉE)
LANG-09	La ***solution du SGDSL*** devrait prendre en charge l'affichage, la recherche et la capture du jeu de caractères ISO 8859-1 (en particulier les caractères français canadiens).
LANG-10	La ***solution du SGDSL*** devrait prendre en charge un clavier bilingue canadien.

3.4 SECTION C – EXIGENCES DU PORTAIL

3.4.1 Objectif

La ***solution du SGDSL*** doit desservir les ressources internes du Bureau de la traduction, les ressources externes ainsi que les ministères et organismes du gouvernement du Canada (clients). Il devrait fournir des modèles prêts à l'emploi qui peuvent être utilisés et modifiés pour permettre aux clients (ressources internes et externes en fonction de leurs permissions, droits d'accès et rôles) un accès sécurisé à l'information, aux caractéristiques et aux fonctionnalités de la ***solution du SGDSL*** et aux outils de traduction, de terminologie et d'interprétation.

Les fonctionnalités du portail visent à établir un environnement sûr, fiable et accessible pour toutes les ressources internes du Bureau de la traduction, les **fournisseurs** externes et les ***fournisseurs de services linguistiques***, les ministères et organismes du gouvernement du Canada (clients), tel que décrit dans les diverses sections de l'énoncé des travaux.

3.4.2 Exigences

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
PRTL-CLNT-01	La solution doit disposer d'un portail client sécurisé, basé sur le Web et personnalisable.

SECTION DE L'EDT	Exigence (COTÉE)
Généralités La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	
PRTL-GEN-02.1	Permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de créer, modifier, supprimer, consulter et publier du contenu dans le portail.
PRTL-GEN-02.2	Permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de consulter dans le portail les notifications en vigueur ou expirées du système.
PRTL-GEN-02.3	Permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de créer et de configurer des notifications contextuelles pour les mises à jour des comptes-clients, les ressources internes du Bureau de la traduction ainsi que les mises à jour des profils des ressources externes et de l'information.
PRTL-LANG-03	La ***solution du SGDSL*** devrait être dotée d'une interface de portail bilingue complète pour tous les utilisateurs (internes et externes) qui comprend de l'information, de la formation et du soutien, et qui présente à tous les utilisateurs un aperçu pertinent à leurs rôles et responsabilités.
PRTL-CONT-04	**Contenu et données** La ***solution du SGDSL*** devrait permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de créer, de modifier, de supprimer, d'examiner, d'approuver et de publier du contenu dans le portail.

SECTION DE L'EDT	Exigence (COTÉE)
PRTL-LAND-05	**Page de renvoi** La ***solution du SGDSL*** devrait permettre la création et la configuration de pages précises d'un site Web destinées aux clients permettant par exemple a) de s'inscrire pour créer un profil d'utilisateur; b) de transmettre des communications pertinentes; c) de fournir des renseignements sur les particularités du SGDSL; d) de permettre une ouverture de session unique pour les utilisateurs du GC et d'avoir un accès authentifié à toutes les composantes du SGDSL en fonction des permissions, des droits d'accès et des rôles des utilisateurs.
PRTL-DASH-06	**Tableaux de bord** La ***solution du SGDSL*** devrait fournir l'accès à des tableaux de bords incluant les fonctionnalités et informations suivantes : a) établir des objectifs et des attentes pour des utilisateurs ou des groupes précis; b) souligner les exceptions et générer des alertes lorsque des problèmes surviennent; c) communiquer les progrès et les réussites; d) fournir une interface commune permettant l'interaction avec les données opérationnelles et leur analyse; e) permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de configurer et d'utiliser différents modèles réutilisables comprenant différentes fonctions et commandes, dont la capacité de choisir un tableau de bord parmi différents tableaux de bord configurables; f) permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de structurer leurs tableaux de bord; g) permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de visualiser, de rechercher et d'organiser (p. ex. trier et filtrer) leurs activités professionnelles.
Ouverture de session La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	
PRTL-LOGN-07.1	Fournir un accès sécurisé aux clients, aux ressources internes et aux ressources externes en fonction des normes de sécurité des TI du GC et des profils de contrôle de la sécurité.
PRTL-LOGN-07.2	Configurer et permettre une ouverture de session unique pour les ressources du GC et assurer, en fonction des permissions, des droits d'accès et des rôles, un accès contrôlé aux caractéristiques, aux fonctionnalités et aux outils de la ***solution du SGDSL***.
PRTL-LOGN-07.3	Fournir aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de configuration et de gestion, des fonctions d'ouverture de session, de libre-service, et d'inscription de clients, de ressources internes et de ressources externes ainsi qu'un guide d'aide de l'utilisateur, une foire aux questions et toute autre forme de formation en ligne.
PRTL-LOGN-07.4	Configurer les modalités d'utilisation du SGDSL pour qu'elles s'affichent à diverses étapes prédéfinies du processus afin de confirmer l'acceptation du SGDSL (affichage répété configurable).
Communication La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	

SECTION DE L'EDT	Exigence (COTÉE)
PRTL-COMM-08.1	Permettre et faciliter la communication entre les ressources internes, les ressources externes et les ministères et organismes du GC (clients).
PRTL-COMM-08.2	Permettre aux utilisateurs d'accéder à toutes les communications électroniques dans ***la solution du SGDSL*** des ressources internes, des ***fournisseurs*** et ***fournisseurs de services linguistiques externes***, et des ministères et organismes du GC.
PRTL-COMM-08.3	Configurer le message de notification et le diffuser en suivant les étapes établies du flux de travaux du SGDSL (p. ex. demandes d'approbation, état de la facture ou réception des biens, note de crédit).
PRTL-COMM-08.4	Aviser les utilisateurs lorsque les clients ont accusé réception de leurs demandes (p. ex. demandes de prix), de leurs commandes (demandes) et de leurs messages dans ***la solution du SGDSL***.
PRTL-COMM-08.5	Permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de créer des messages électroniques sortants et de les transmettre aux utilisateurs du portail.
PRTL-COMM-08.6	Communiquer avec tous les utilisateurs du portail ou à un sous-ensemble d'utilisateurs du portail (p. ex. être capable de créer des listes de distribution des courriels).
Client du TB La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	
PRTL-CLNT-09.1	Soumettre des demandes de service en ligne.
PRTL-CLNT-09.2	Visualiser l'état d'avancement des demandes de service en ligne en temps réel tout au long du flux des travaux.
PRTL-CLNT-09.3	Aviser lorsque la date d'achèvement des demandes de service a été modifiée.
PRTL-CLNT-09.4	Rechercher, filtrer, visualiser, télécharger, imprimer et sauvegarder les demandes de service passées et actuelles.
PRTL-CLNT-09.5	Rechercher, filtrer, visualiser, télécharger, imprimer et sauvegarder les soumissions passées et actuelles pour les travaux à effectuer.
PRTL-CLNT-09.6	Rechercher, filtrer, visualiser, télécharger, imprimer et sauvegarder la facturation des demandes de service passées et actuelles.
PRTL-CLNT-09.7	Ajouter des commentaires aux demandes de service actives soumises en ligne dans la ***solution du SGDSL*** tout au long du flux des travaux.
PRTL-CLNT-09.8	Communiquer avec les ressources du Bureau de la traduction dans le cadre des demandes de service actives soumises en ligne dans la ***solution du SGDSL*** tout au long du flux des travaux.
PRTL-CLNT-09.9	Configurer les paramètres pour générer des rapports passés et actuels sur les demandes de service, les devis et les factures.
PRTL-CLNT-09.10	Télécharger les documents de référence.
PRTL-CLNT-09.11	Créer des demandes de service et télécharger les documents Protégé A et B.
PRTL-CLNT-09.12	Créer des demandes de service pour toutes les catégories de classe d'information.
PRTL-CLNT-09.12.1	Restreindre le téléchargement des documents classifiés de niveau supérieur à Protégé B.
PRTL-CLNT-09.13	Permettre de restreindre l'accès aux caractéristiques et fonctionnalités en fonction du rôle, des droits d'accès et des permissions.
Ressources internes du Bureau de la traduction La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	

SECTION DE L'EDT	Exigence (COTÉE)
PRTL-INTRES-10.1	Communiquer avec les ressources du Bureau de la traduction dans le cadre des demandes actives (projet) soumises en ligne dans la ***solution du SGDSL*** tout au long du flux des travaux.
PRTL-INTRES-10.2	Récupérer la trousse de traduction, par exemple, le texte source et les documents de référence.
PRTL-INTRES-10.3	Visualiser et afficher la progression des tâches et des activités dans le cadre de toutes les demandes actives (**projet**).
PRTL-INTRES-10.4	Rechercher, filtrer et générer des rapports sur les demandes (**projet**), notamment les tâches actives, annulées, livrées et inactives.
PRTL-INTRES-10.5	Télécharger les documents traduits et les documents de référence.
PRTL-INTRES-10.6	Visualiser les charges de travail en temps réel.
PRTL-INTRES-10.7	Visualisez les charges de travail en temps réel sur un appareil mobile.
PRTL-INTRES-10.8	Rechercher, filtrer, visualiser, télécharger, imprimer et sauvegarder le calendrier et les horaires.
Ressources externes La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	
PRTL-EXTRES-11.1	Communiquer avec les ressources du Bureau de la traduction dans le cadre des demandes actives (**projet**) soumises en ligne dans la ***solution du SGDSL*** tout au long du flux des travaux.
PRTL-EXTRES-11.2	Visualiser et afficher la progression des tâches et des activités dans le cadre de toutes les demandes actives (**projet**).
PRTL-EXTRES-11.3	Rechercher, filtrer et générer des rapports sur les demandes (**projet**), notamment les tâches actives, annulées, livrées et inactives.
PRTL-EXTRES-11.4	Rechercher, filtrer, visualiser, télécharger, imprimer et sauvegarder la facturation des demandes de service passées et actuelles.
PRTL-EXTRES-11.5	Télécharger les documents traduits et les documents de référence.
PRTL-EXTRES-11.6	Permettre d'entrer le temps réel par tâche pour la traduction, la terminologie et l'interprétation.
PRTL-EXTRES-11.7	Visualiser les charges de travail en temps réel.
PRTL-EXTRES-11.8	Rechercher, filtrer, visualiser, télécharger, imprimer et enregistrer les notes d'évaluation passées et actuelles.
PRTL-EXTRES-11.9	Rechercher, filtrer, visualiser, télécharger, imprimer et sauvegarder le calendrier et les horaires.
PRTL-EXTRES-11.10	Permettre l'accès à des ressources externes pour récupérer le travail et retourner les documents de référence, le texte traduit et les autres documents.

3.5 SECTION D – GESTION DU FLUX DE TRAVAUX

3.5.1 Objectif

La solution du SGDSL doit permettre de configurer les tâches et les activités dans le cadre du flux des travaux qui peut nécessiter une intervention manuelle, être semi-automatique et entièrement automatisé, afin de gérer l'ensemble des flux de processus de bout en bout et les services de traduction, de terminologie et d'interprétation du Bureau de la traduction. Il doit couvrir la soumission d'un **projet** (demande), la prestation du service et la facturation.

3.5.2 Exigences

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
WF-01	L'entrepreneur doit fournir une solution qui fournit le mécanisme pour construire, configurer et adapter les flux de travaux.

SECTION DE L'EDT	Exigence (COTÉE)
La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	
WF-02	Fournir aux utilisateurs des renseignements sur les erreurs pendant la création du flux de travaux ainsi que des renseignements expliquant pourquoi un flux de travaux ne peut pas être réalisé.
WF-03	Créer, modifier, supprimer, configurer et tester des flux de travaux qui incluent des flux de travaux manuels, semi-automatisés et entièrement automatisés.
WF-04	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés a) de créer, d'ajouter, de modifier et supprimer des tâches de **projet** dans un flux de travaux manuel, semi-automatisé et entièrement automatisé, qu'il soit séquentiel ou parallèle; b) de personnaliser, configurer et gérer des activités et des tâches de **projet** dans un flux de travaux manuel, semi-automatisé et entièrement automatisé, qu'il soit séquentiel ou parallèle; c) d'ajouter des activités et des tâches de **projet** supplémentaires à un flux de travaux particulier, peu importe l'intervalle, que le flux soit séquentiel ou parallèle, notamment à l'appui des fonctions et des évaluations de la qualité des documents; d) d'établir des règles opérationnelles et de validation pour des flux de travaux manuels, semi-automatisés et entièrement automatisés.
WF-05	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer ce qui suit a) les flux de travaux de bout en bout depuis la soumission du **projet** client (demande) jusqu'à la livraison et la facturation; b) le processus d'approbation du flux de travaux; c) les états des flux de travaux; d) les notifications du flux de travaux e) le responsable (groupe ou personne); f) la mesure requise (observation, approbation/rejet ou modification/approbation/rejet); g) la liste de raisons acceptables justifiant l'approbation ou le rejet; h) les règles d'acheminement à l'échelon supérieur (durée de l'inactivité, groupe ou personne à qui transmettre l'information).
WF-06	Gérer les échéances du **projet**.
WF-07	Consulter l'état des tâches du **projet** dans le flux de travaux en temps réel.
WF-08	Ajouter, modifier ou supprimer des commentaires relatifs au **projet** dans son ensemble et aux tâches du **projet** dans le flux de travaux.
WF-09	Conserver l'historique de tous les commentaires du **projet** et des tâches du **projet** qui ont été ajoutés, modifiés ou supprimés avec l'identificateur d'utilisateur ainsi que l'horodatage.

SECTION DE L'EDT	Exigence (COTÉE)
WF-10	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer le délai d'exécution d'une tâche ou d'une activité.
WF-11	Permettre le suivi de la réception et du traitement des tâches et des activités liées au soutien requis.
WF-12	Permettre d'automatiser la préparation d'une trousse à l'intention des ressources externes comprenant d'autres documents à traduire, des extraits pertinents de la MT, le rapport d'analyse et la documentation de référence.

3.6 SECTION E – GESTION DE LA CHARGE DE TRAVAIL

3.6.1 Objectifs

La ***solution du SGDSL*** doit comprendre une composante de gestion de la charge de travail qui peut être utilisée pour gérer les ressources internes du Bureau de la traduction et les ressources externes pour la traduction, la terminologie, l'interprétation et le soutien connexe, ce qui peut comprendre la correction d'épreuves, la publication assistée par ordinateur et les services de documentation. Elle assurera la visibilité nécessaire pour planifier, organiser et distribuer plus efficacement la charge de travail des ressources ainsi qu'établir le calendrier manuellement ou automatiquement.

3.6.2 Exigences

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
WL-MAN-01	La ***solution du SGDSL*** doit comporter des fonctions de gestion de la charge de travail.
WL-MAN-02	La ***solution du SGDSL*** doit permettre à un utilisateur ayant les permissions, les droits d'accès et les rôles appropriés de configurer les paramètres et les coefficients de la convention collective utilisés pour calculer le nombre total d'heures travaillées par un interprète (voir la partie 12, Appendice E – Exemple et calcul de la charge de travail d'interprétation).

SECTION DE L'EDT	Exigence (COTÉE)
WL-03	La ***solution du SGDSL*** devrait inclure la capacité de planification de la charge de travail suivante : interface Web, capacité d'afficher et de visualiser un ou plusieurs calendriers de ressources en fonction de permissions, les droits d'accès et des rôles de l'utilisateur, et capacité d'interagir avec le calendrier.
WL-04	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de définir et de configurer les priorités, la validation et les règles opérationnelles des calendriers de la charge de travail.
WL-05	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de mettre à jour et de supprimer un calendrier de charge de travail.
WL-06	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de planifier ce qui suit : a) les tâches; b) les événements; c) les ressources locales et les ressources dans différents fuseaux horaires; d) la restauration;

SECTION DE L'EDT	Exigence (COTÉE)
	e) l'équipement; f) les salles de réunions, g) l'attribution de postes de travail.
WL-07	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de sélectionner ou de saisir le type d'absence dans le calendrier de la charge de travail, et d'en faire le suivi, en plus d'inclure ce qui suit : a) la formation; b) les congés (de maladie, pour raisons personnelles ou de famille, de maternité et parentaux); c) les affectations à plein temps et à temps partiel; d) les absences pour rendez-vous; e) les jours fériés; f) les vacances; g) le retour progressif; h) les heures supplémentaires.
WL-08	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de diffuser le plus récent calendrier de la charge de travail.
WL-09	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer le calendrier de la charge de travail.
WL-10	La ***solution du SGDSL*** devrait permettre de diffuser le calendrier de la charge de travail manuellement et automatiquement dans un délai configurable.
WL-11	La ***solution du SGDSL*** devrait assurer le suivi des changements apportés au calendrier de la charge de travail en fonction de l'identificateur ou de nom d'utilisateur, de l'horodatage et de la description.
WL-12	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter des commentaires facultatifs aux tâches.
WL-13	La ***solution du SGDSL*** devrait conserver l'historique de commentaires de la tâche avec l'identificateur ou le nom d'utilisateur et l'horodatage.
WL-14	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter des liens vers des documents de référence à une tâche.
WL-15	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de mettre à jour un calendrier de charge de travail en temps réel.
WL-16	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de consulter le calendrier de la charge de travail d'une seule ressource ou de plusieurs ressources.
WL-17	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'imprimer le calendrier de la charge de travail d'une seule ressource ou de plusieurs ressources.

SECTION DE L'EDT	Exigence (COTÉE)
WL-18	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de rechercher et de filtrer les ressources selon ce qui suit : a) la disponibilité; b) les compétences; c) les domaines de spécialisation; d) le profil linguistique; e) la cote de sécurité; f) les clients; g) les ressources internes du Bureau de la traduction ou les ressources externes (FSL); h) le contrat; i) l'emplacement.
WL-19	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de sauvegarder des recherches et des filtres pour une utilisation ultérieure.
WL-20	La ***solution du SGDSL*** devrait permettre aux ressources d'ouvrir une session pour consulter un ou plusieurs calendriers selon les permissions, les droits d'accès et les rôles de l'utilisateur.
WL-21	La ***solution du SGDSL*** devrait permettre à une seule ressource détenant les permissions, les droits d'accès et les rôles appropriés de saisir, de modifier, de supprimer et de consulter les heures et les dépenses.
WL-22	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de saisir les heures en blocs, notamment pour les vacances et la formation.
WL-23	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de saisir, de modifier, de supprimer, de consulter et d'approuver les heures et les dépenses (de toute sorte).
WL-24	La ***solution du SGDSL*** devrait permettre le suivi des heures des clients ou des projets et comparer les heures de projet facturables par rapport aux heures de projet non facturables ou au compte de mots d'un projet.
WL-25	La ***solution du SGDSL*** devrait permettre la comparaison des heures prévues d'une ressource aux heures réelles déclarées.
WL-26	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de préciser la plage de dates pour produire des rapports de calendrier de charge de travail prédéfinis et personnalisés.
WL-27	La ***solution du SGDSL*** devrait permettre la définition et la configuration d'alertes et d'avertissements automatisés pour signaler : a) la date d'expiration des attestations, des contrats et des tarifs; b) les conflits d'affectation des ressources; c) les dates d'échéance et les seuils budgétaires qui approchent; d) la sous-utilisation ou surutilisation éventuelle des ressources.
WL-28	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de mettre en place des rappels.
WL-29	La ***solution du SGDSL*** devrait fournir des interfaces de programmation d'applications (IPA) pour les applications de calendrier tiers.

SECTION DE L'EDT	Exigence (COTÉE)
WL-30	La ***solution du SGDSL*** doit permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de restreindre l'affichage et l'accès aux caractéristiques et aux fonctionnalités.
WL-31	La ***solution du SGDSL*** devrait fournir des indicateurs d'état visuels pour ce qui suit : a) les progrès des tâches; b) l'utilisation des ressources; c) la disponibilité.
WL-32	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'établir et de configurer la planification des ressources en fonction des fuseaux horaires du Canada.
WL-33	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de planifier le travail des ressources dans tous les fuseaux horaires du Canada.
WL-34	La ***solution du SGDSL*** devrait indiquer à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés qu'une ressource de trouve dans un autre fuseau horaire du Canada.
WL-35	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer un profil de client qui contient : un compte, des coordonnées, des lexiques approuvés par le client, des préférences, des guides de rédaction, des documents de référence, les coordonnées de l'approbateur, les méthodes de communication et de correspondance, par exemple, courriel, téléphone, instructions spéciales (courantes, le plus souvent demandées).
WL-36	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer des profils de ressources internes du Bureau de la traduction qui contiennent des rôles, des qualifications, des certifications, des profils linguistiques, des autorisations de sécurité, des fuseaux horaires du Canada, des domaines de traduction et des spécialités (terminologie aéronautique, médicale, etc.)
WL-37	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer des profils de ressources externes qui contiennent des domaines d'expertise, de l'information contractuelle, des numéros de contrats, des coordonnées, des ensembles de compétences, des spécialisations, des niveaux d'autorisation de sécurité, des langues de travail (interprétation), des notes d'évaluation, des calendriers et des échéanciers de ressources, le nombre de mots résiduels qu'il reste au contrat (et des tarifs).
WL-38	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer l'échelle de mots ayant servi à calculer le nombre d'heures aux fins de facturation et le nombre d'heures prévues pour l'exécution en fonction du service demandé par le client (p. ex., traduction de 214 mots/heure et révision de 856 mots/heure).
WL-39	La ***solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer les

SECTION DE L'EDT	Exigence (COTÉE)
	taux de facturation des clients qui sont utilisés pour calculer la facture pour les travaux réalisés.
WL-40	La ***solution du SGDSL*** devrait permettre un suivi en temps réel de la capacité journalière des ressources externes de traduction et du nombre de mots/heures restant dans le contrat.
WL-41	La ***solution du SGDSL*** doit pouvoir générer manuellement et automatiquement un document contenant les informations nécessaires à l'attribution du travail à une ressource externe, par exemple, une autorisation de tâches.

3.7 SECTION F – TRADUCTION ASSISTÉE PAR ORDINATEUR (TAO)

3.7.1 Objectifs

La traduction assistée par ordinateur (TAO) est un élément clé du Bureau de la traduction qui est essentiel à son succès et à son efficience. Elle est utilisée pour exécuter et accélérer le processus de livraison d'une demande de traduction qui comprend généralement : la demande du client du TB, la préparation du fichier source, l'analyse et le prétraitement, la traduction, y compris des fonctions d'appui comme la relecture et la vérification de l'orthographe, les vérifications, la livraison au client du TB et la facturation du client du TB. Plusieurs des entrepreneurs en TAO proposent une gamme d'outils comme des analyseurs, des éditeurs, des mémoires de traduction (MT), des outils d'alignement, des concordanciers, des outils de traduction automatique, des bases de données terminologiques, des extracteurs terminologiques, des outils d'assurance de la qualité et des outils de localisation. De plus, certains entrepreneurs proposent également des volets de gestion de **projets** (demandes), des systèmes de gestion du contenu (SGC) et des IPA qui permettent la connexion à des outils tiers ainsi que des outils de gestion du flux de travaux et de la charge de travail. Tous ces outils combinés fournissent une suite complète qui permettra au Bureau de la traduction d'avancer.

3.7.2 Aperçu

3.7.2.1 Analyseur

L'analyseur est un outil qui sert à estimer les efforts requis d'un traducteur pour la traduction d'un document et à fournir au client du TB une estimation des coûts pour la traduction du document. L'analyseur effectue une analyse du document à traduire en le comparant à une mémoire de traduction (MT) et à un corpus. Il fournit les renseignements suivants :

a) le compte de mots total;
b) les correspondances exactes (100 %) – le nombre et/ou le pourcentage de mots, de caractères ou de segments pour lesquels une correspondance à 100 % a été trouvée;
c) les correspondances floues – le nombre et/ou le pourcentage de mots, de caractères ou de segments pour lesquels une correspondance inférieure à 100 % a été trouvée (le degré de la correspondance est indiqué par le pourcentage);
d) les répétitions – le nombre et/ou le pourcentage de mots, de caractères ou de segments qui sont des répétitions de mots déjà comptés;

e) les correspondances de contexte – le nombre et/ou le pourcentage de mots, de caractères ou de segments pour lesquels une correspondance de contexte a été trouvée.

3.7.2.2 Éditeur

L'éditeur est l'outil de TAO que les traducteurs utilisent pour ouvrir un fichier source aux fins de traduction et pour interroger la mémoire et les bases de données terminologiques afin de récupérer les données pertinentes. Il s'agit également de l'espace de travail dans lequel les traducteurs peuvent saisir leurs propres traductions si aucune correspondance n'est trouvée, ainsi que de l'interface pour verser les phrases (segments) traduites dans la mémoire de traduction ainsi que les termes appariés dans la base de données terminologiques.

3.7.2.3 Mémoire de traduction

Une mémoire de traduction (MT) est une base de données qui contient les traductions antérieures, qui ont été alignées et qui sont prêtes à être utilisées de nouveau dans les segments sources et cibles correspondants. Ces traductions sont habituellement délimitées par une ponctuation explicite; il s'agit généralement d'une phrase, mais il peut également s'agir d'un titre, d'une légende ou du contenu d'une cellule de tableau. Une entrée type de MT est un segment source lié à sa traduction, ainsi que les métadonnées pertinentes (p. ex., heure/date et nom de l'auteur, nom du client du TB, sujet, etc. L'application de MT contient également l'algorithme pour récupérer une traduction correspondante si le même segment ou un segment semblable est présent dans un nouveau texte. La majorité des ***solutions disponibles sur le marché*** peuvent importer ou exporter des mémoires en utilisant le format Translation Memory eXchange (TMX), une norme XML ouverte créée par OSCAR (Open Standards for Container/Content Allowing Re-use), un groupe d'intérêt spécial de LISA (Localization Industry Standards Association).

3.7.2.4 Alignement

L'alignement permet d'utiliser les traductions précédentes en transformant les documents traduits précédemment en segments de traduction afin que ces derniers puissent être ajoutés à une mémoire de traduction (MT). L'outil d'alignement fait correspondre les fichiers de langue source et de langue cible côte à côte, afin de déterminer quelles paires vont ensemble. Une fois le processus terminé, le document est envoyé pour vérification afin de s'assurer que tous les segments et leurs correspondances sont corrects et de corriger (ou supprimer, si nécessaire) les paires incorrectes. Les outils d'alignement comprennent certaines fonctions d'édition et de surveillance afin de permettre de diviser ou de fusionner les segments au besoin, et de détecter les segments incomplets ou en trop, pour assurer une correspondance 1:1 parfaite entre les deux documents. La norme ouverte LISA/OSCAR Segmentation Rules eXchange (SRX) a été créée pour optimiser le rendement d'un système à l'autre.

3.7.2.5 Concordancier

La concordance est une façon d'évaluer un corpus de texte pour montrer comment un mot ou une phrase donnée dans le texte est utilisé dans les contextes immédiats dans lesquels il apparaît. Les concordances sont fréquemment utilisées en linguistique dans le cadre de l'étude d'un texte. Un concordancier typique permettrait à une personne de saisir un mot ou une phrase et d'effectuer une recherche pour trouver plusieurs exemples de la façon dont le mot ou la phrase est utilisé couramment dans un discours ou par écrit.

3.7.2.6 Traduction automatique

La traduction automatique (TA) est une traduction automatisée ou une traduction réalisée par un ordinateur. Il s'agit d'un processus, parfois appelé « traitement du langage naturel » qui utilise un ensemble de données bilingues et d'autres actifs linguistiques pour établir des modèles linguistiques ou de phrases servant à traduire un texte. Le résultat est souvent une traduction approximative qui est incorrecte et non grammaticale, et qui exige habituellement une post-édition par une personne, mais qui est moins chère/plus rapide à corriger qu'une traduction à partir de zéro. La TA peut également être utilisée de façon interactive : pendant qu'un traducteur traduit dans un outil de TAO, la TA présente des suggestions.

3.7.2.7 Bases de données terminologiques

Les bases de données terminologiques sont semblables aux MT qui contiennent des segments réutilisables, mais fonctionnent au niveau des termes en gérant des glossaires consultables/récupérables qui contiennent des paires spécifiques de termes sources et cibles ainsi que les métadonnées connexes. La base de données terminologiques vérifie le segment de la traduction active dans l'éditeur en fonction du contenu d'une base de données, comme un glossaire bilingue, et lorsqu'elle détecte une correspondance du terme source, elle propose l'équivalence cible correspondante. Une base de données terminologique peut contenir divers glossaires divisés selon différents critères, comme les domaines, les spécialisations, les clients du TB et les projets. Pour faciliter et améliorer la capacité d'échange, une norme ouverte Terminology Base eXchange (TBX) a été créée par OSCAR/LISA. De nos jours, les systèmes les plus évolués sont conformes à la norme TBX.

3.7.2.8 Extraction terminologique

Le but de l'extraction terminologique est d'extraire automatiquement les termes pertinents d'un corpus donné. Les termes peuvent être extraits soit manuellement ou en surlignant les mots dans des documents et en les transférant dans un programme, comme Word ou Excel, ou automatiquement, en utilisant des outils d'extraction terminologique. La norme qui définit un cadre fondé sur le XML pour la représentation des données terminologiques structurées est appelée TermBase eXchange (TBX).

3.7.2.9 Assurance de la qualité (AQ)

Les modules d'assurance de la qualité (AQ) effectuent des contrôles linguistiques en vérifiant l'usage de la terminologie, l'orthographe et la grammaire, et en confirmant que tous les éléments non traduisibles (p. ex., certains noms propres) demeurent inchangés. Ils peuvent également détecter si les nombres, les mesures et les devises sont correctement indiqués selon les conventions de la langue cible. Sur le plan technique, ils assurent qu'aucun segment cible n'est laissé non traduit et que les balises de format cible correspondent aux balises sources en ce qui a trait au type et à la quantité. Une fois les conditions de la liste de contrôle d'AQ remplies, le document peut être exporté en toute confiance vers son format d'origine pour la relecture finale et la diffusion.

3.7.2.10 Exigences

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
CAT-MAN-01	***La solution du SGDSL*** doit être doté d'une suite d'outils de TAO qui comprend un analyseur, un éditeur, une mémoire de traduction, une base de données terminologiques, un outil de traduction automatique et des modules d'assurance de la qualité.

SECTION DE L'EDT	Exigence (COTÉE)
Généralités (système = outils de TAO) ***La solution du SGDSL*** devrait comporter les capacités suivantes :	
CAT-GEN-02.1	***La solution du SGDSL*** devrait être accessible en ligne et hors ligne.
CAT-GEN-02.2	***La solution du SGDSL*** devrait être offert dans les deux langues officielles (en anglais et en français).
CAT-GEN-02.3	***La solution du SGDSL*** devrait permettre à un utilisateur d'ajouter, de modifier ou de supprimer des commentaires.
CAT-GEN-02.4	***La solution du SGDSL*** devrait conserver l'historique de tous les commentaires ajoutés, modifiés et supprimés ainsi que le code d'utilisateur et l'horodatage.

SECTION DE L'EDT	Exigence (COTÉE)
CAT-GEN-02.5	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de restreindre l'accès aux caractéristiques et aux fonctionnalités.
CAT-GEN-02.6	***La solution du SGDSL*** devrait comprendre plusieurs langues.
CAT-GEN-02.7	***La solution du SGDSL*** devrait fournir une liste de métadonnées prédéfinies et personnalisables.
CAT-GEN-02.8	***La solution du SGDSL*** devrait fournir des fonctions de recherche personnalisables.
CAT-GEN-02.9	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'examiner un document entrant afin d'établir l'effort et les coûts associés à sa traduction et inclure ce qui suit : a) le nettoyage; b) la prétraduction; c) le compte de mots; d) la traduction de la terminologie; e) la création d'une trousse de texte; f) la reconnaissance optique de caractères (ROC) (format PDF).
Analyseur ***La solution du SGDSL*** devrait comporter les capacités d'analyseur suivantes :	
CAT-ANLZ-03.1	***La solution du SGDSL*** devrait permettre le téléchargement manuel des documents.
CAT-ANLZ-03.2	***La solution du SGDSL*** devrait permettre le téléchargement automatique des documents.
CAT-ANLZ-03.3	***La solution du SGDSL*** devrait permettre le traitement des types de format suivants : a) MS Word (doc, docx), b) MS Excel (xls, xlsx), c) MS Power Point (ppt, pptx), d) PDF; e) MS Visio (vsd).
CAT-ANLZ-03.4	***La solution du SGDSL*** devrait permettre la numérisation des documents.
CAT-ANLZ-03.5	***La solution du SGDSL*** devrait permettre la conversion des types de documents suivants : a) MS Word (doc, docx), b) Txt, c) Odt; d) Wpd.
La solution du SGDSL devrait fournir un rapport d'analyse basé sur les segments.	
CAT-ANLZ-03.6.1	L'information du rapport d'analyse devrait contenir ce qui suit : a) le nom et l'extension du fichier; b) le compte de mots – nombre de redondances, nombre de nouveaux mots, total; c) le nombre de segments – nombre de redondances, nombre de nouveaux segments, total; d) le nom ou le numéro du ***projet***; e) le nombre de dossiers.
CAT-ANLZ-03.6.2	Les détails de l'analyse de la distribution des mots devraient comprendre ce qui suit : a) exact – nombre de mots, pondération en pourcentage; b) flou – nombre de mots, pondération en pourcentage; c) répétition – nombre de mots, pondération en pourcentage; d) nouveau – nombre de mots, pondération en pourcentage;
CAT-ANLZ-03.7	***La solution du SGDSL*** devrait permettre la configuration des correspondances floues.

SECTION DE L'EDT	Exigence (COTÉE)
CAT-ANLZ-03.8	***La solution du SGDSL*** devrait permettre d'inclure les éléments suivants de MS Word dans le compte de mots de l'analyseur : a) les marques de révisions (suivi des modifications); b) les zones de texte (encadrés, boîtes de texte); c) les tables des matières (codes de champs et manuelles); d) les en-têtes et les pieds de page; e) les notes de bas de page; f) les notes en fin de texte; g) les références; h) les tableaux; i) les graphiques faits avec un logiciel d'édition.
CAT-ANLZ-03.9	***La solution du SGDSL*** devrait permettre d'inclure les éléments suivants de MS PowerPoint dans le compte de mots de l'analyseur : a) les pages de notes; b) les masques des diapositives; c) les graphiques produits et sauvegardés avec un logiciel d'édition; d) les en-têtes et les pieds de page; e) les zones de texte; f) les tableaux.
CAT-ANLZ-03.10	***La solution du SGDSL*** devrait permettre d'inclure les éléments suivants de MS Excel dans le compte de mots de l'analyseur : a) les onglets multiples; b) le nom donné à l'onglet; c) le contenu masqué (cellules, colonnes, lignes, onglets); d) les commentaires; e) les marques de révisions; f) le texte masqué; g) les zones de texte; h) les menus déroulants; i) les tableaux.
CAT-ANLZ-03.11	***La solution du SGDSL*** devrait permettre d'inclure les éléments suivants de MS Visio dans le compte de mots de l'analyseur : les onglets multiples.
CAT-ANLZ-03.12	***La solution du SGDSL*** devrait permettre d'inclure les éléments suivants d'Adobe PDF dans le compte de mots de l'analyseur : le format texte – contenu éditable.
CAT-ANLZ-03.13	***La solution du SGDSL*** devrait afficher le contenu du fichier à traduire, divisé en segments.
CAT-ANLZ-03.14	***La solution du SGDSL*** devrait afficher les langues sources et cibles.
CAT-ANLZ-03.15	***La solution du SGDSL*** devrait afficher une liste numérotée des segments sources.
CAT-ANLZ-03.16	***La solution du SGDSL*** devrait afficher les segments sources et leurs équivalences cibles côte à côte.
CAT-ANLZ-03.17	***La solution du SGDSL*** devrait indiquer l'état du segment source : i. exact, ii. flou, iii. répétition, iv. nouveau.
CAT-ANLZ-03.18	***La solution du SGDSL*** devrait indiquer le pourcentage de correspondance du segment équivalent cible.

SECTION DE L'EDT	Exigence (COTÉE)
CAT-ANLZ-03.19	***La solution du SGDSL*** devrait permettre la sauvegarde du rapport d'analyse.
CAT-ANLZ-03.20	***La solution du SGDSL*** devrait permettre l'impression du rapport d'analyse.
CAT-ANLZ-03.21	***La solution du SGDSL*** devrait afficher des messages d'erreur si le rapport d'analyse ne peut être produit.
CAT-ANLZ-03.22	***La solution du SGDSL*** devrait afficher des messages d'erreur si le rapport d'analyse est incomplet.
CAT-ANLZ-03.23	***La solution du SGDSL*** devrait indiquer si le document téléchargé manuellement ou automatiquement est protégé par un mot de passe.
CAT-ANLZ-03.24	***La solution du SGDSL*** devrait permettre la configuration des règles entourant le compte de mots en fonction des éléments suivants : a) les types de caractères; b) les chiffres; c) les symboles.
CAT-ANLZ-03.25	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'établir les paramètres d'estimation du nombre d'heures de travail nécessaire pour effectuer la traduction en fonction du nombre de mots pondérés.
CAT-ANLZ-03.26	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'établir les paramètres pour estimer le coût de la demande de traduction d'un client du TB en fonction des tarifs et du nombre de mots pondérés.
CAT-ANLZ-03.27	***La solution du SGDSL*** devrait permettre l'exportation du rapport d'analyse dans les formats suivants : a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) XML, e) CSV.
CAT-ANLZ-03.28	***La solution du SGDSL*** devrait permettre d'afficher le rapport d'analyse dans un navigateur.
CAT-ANLZ-03.29	***La solution du SGDSL*** devrait détecter la langue source.
CAT-ANLZ-03.30	***La solution du SGDSL*** devrait détecter les images.
Éditeur ***La solution du SGDSL*** devrait comporter les fonctionnalités d'éditeur suivantes :	
CAT-EDIT-04.1	***La solution du SGDSL*** doit être accessible en ligne et hors ligne.
CAT-EDIT-04.2	***La solution du SGDSL*** devrait avoir une interface-utilisateur configurable.
CAT-EDIT-04.3	***La solution du SGDSL*** devrait permettre la conversion d'une page Web HTML (HyperText Markup Language) vers un document Word afin de travailler hors ligne.
CAT-EDIT-04.4	***La solution du SGDSL*** devrait permettre la traduction de multiples types de formats de documents.
CAT-EDIT-04.5	***La solution du SGDSL*** devrait permettre à un utilisateur de sélectionner la façon dont les segments sources et cibles sont affichés.
CAT-EDIT-04.6	***La solution du SGDSL*** devrait être dotée des capacités suivantes : a) recherche et remplacement; b) suppression; c) annulation des modifications; d) tri; e) fusion;

SECTION DE L'EDT	Exigence (COTÉE)
	f) gestion du marquage; g) surlignement avancé; h) suggestion automatique.
CAT-EDIT-04.7	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de restreindre l'accès aux caractéristiques et aux fonctionnalités.
CAT-EDIT-04.8	***La solution du SGDSL*** devrait permettre la traduction de multiples documents simultanément.
CAT-EDIT-04.9	***La solution du SGDSL*** devrait comporter un éditeur tel-tel.
CAT-EDIT-04.10	***La solution du SGDSL*** devrait permettre l'édition de texte enrichi.
CAT-EDIT-04.11	***La solution du SGDSL*** devrait permettre la comparaison des contextes cibles et sources.
CAT-EDIT-04.12	***La solution du SGDSL*** devrait fournir des IPA (interfaces de programmation d'applications) pour les éditeurs tiers.
CAT-EDIT-04.13	***La solution du SGDSL*** devrait permettre à un utilisateur d'ajouter, de modifier ou de supprimer des commentaires dans les segments.
CAT-EDIT-04.14	***La solution du SGDSL*** devrait conserver l'historique de tous les commentaires ajoutés, modifiés ou supprimés ainsi que le nom ou le code d'utilisateur et l'horodatage.
CAT-EDIT-04.15	***La solution du SGDSL*** devrait permettre à un utilisateur de personnaliser les recherches dans l'éditeur à l'aide d'expressions courantes.
CAT-EDIT-04.16	***La solution du SGDSL*** devrait fournir des connecteurs vers les outils d'édition tiers.
CAT-EDIT-04.17	***La solution du SGDSL*** devrait permettre l'utilisation de logiciels de reconnaissance vocale.
CAT-EDIT-04.18	***La solution du SGDSL*** devrait être doté d'une fonctionnalité de traduction rapide des documents en utilisant les mémoires de traduction ou les outils de traduction automatique d'un entrepreneur ou d'un tiers.
CAT-EDIT-04.19	***La solution du SGDSL*** devrait avoir une fonction de concordancier.
CAT-EDIT-04.20	***La solution du SGDSL*** devrait permettre à un utilisateur ayant les permissions, les droits d'accès et les rôles appropriés de configurer des raccourcis clavier pour les caractéristiques et les fonctionnalités.
Mémoire de traduction (MT) ***La solution du SGDSL*** devrait comporter les fonctionnalités de mémoire de traduction suivantes :	
CAT-TM-05.1	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de créer, de modifier et de supprimer une MT.
CAT-TM-05.2	***La solution du SGDSL*** devrait permettre l'importation et l'exportation du contenu de la MT.
CAT-TM-05.3	***La solution du SGDSL*** devrait se conformer à XLIFF 2.0 (XML Localisation Interchange File format).
CAT-TM-05.4	***La solution du SGDSL*** devrait se conformer à TMX 1.4B (Translation Memory Exchange format).
CAT-TM-05.5	***La solution du SGDSL*** devrait permettre la mise à jour en temps réel de la MT.
CAT-TM-05.6	***La solution du SGDSL*** devrait permettre d'effectuer des recherches simultanées dans plusieurs MT.
CAT-TM-05.7	***La solution du SGDSL*** devrait être doté des capacités suivantes : a) recherche et remplacement; b) suppression; c) annulation des modifications; d) tri;

SECTION DE L'EDT	Exigence (COTÉE)
	e) fusion; f) suggestion automatique; g) retrait des éléments en double dans la MT.
CAT-TM-05.8	***La solution du SGDSL*** devrait se conformer à UTF-8 et UTF-16 (forme stockée de caractères).
CAT-TM-05.9	***La solution du SGDSL*** devrait permettre la création d'une MT virtuelle en combinant des MT existantes.
CAT-TM-05.10	***La solution du SGDSL*** devrait également permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de corriger manuellement les segments mal alignés en utilisant notamment les fonctions de fusion, d'échange, d'insertion et de suppression.
CAT-TM-05.11	***La solution du SGDSL*** devrait avoir des fonctions de gestion de MT.
CAT-TM-05.12	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de restreindre l'accès aux caractéristiques et aux fonctionnalités.
CAT-TM-05.13	***La solution du SGDSL*** devrait permettre le stockage manuel et automatique des documents sources originaux, sources mis à jour et cibles finaux, notamment les documents de référence des clients du TB et des fournisseurs.
CAT-TM-05.14	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer la période de conservation en stockage pour les documents sources originaux, sources mis à jour et cibles finaux.
CAT-TM-05.15	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de créer, modifier et supprimer des marquages et des métadonnées pour les documents sources originaux, sources mis à jour et cibles finaux.
CAT-TM-05.16	***La solution du SGDSL*** devrait prendre en charge la numérotation et l'appellation alphanumérique de documents et fichiers stockés.
CAT-TM-05.17	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de créer, modifier et supprimer différents types de MT : *a)* ***projet,*** b) publique, c) privée, d) personnelle, e) clients du TB.
CAT-TM-05.18	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer la période de conservation des MT.
CAT-TM-05.19	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer les paramètres d'épuration automatique et manuelle.
CAT-TM-05.20	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de créer, de modifier et de supprimer des marquages et des métadonnées pour les MT.
CAT-TM-05.21	***La solution du SGDSL*** devrait prendre en charge la numérotation et l'appellation alphanumérique des MT.

SECTION DE L'EDT	Exigence (COTÉE)
CAT-TM-05.22	***La solution du SGDSL*** devrait permettre la conversion manuelle et automatique des documents sources originaux, sources mis à jour et cibles finaux en texte.
CAT-TM-05.23	***La solution du SGDSL*** devrait permettre la conversion en lots manuelle et automatique de documents sources originaux, sources mis à jour et cibles finaux en texte.
CAT-TM-05.24	***La solution du SGDSL*** devrait aviser un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de toute erreur ou de tout échec dans la conversion simple ou en lots de documents sources originaux, sources mis à jour et cibles finaux en texte.
CAT-TM-05.25	***La solution du SGDSL*** devrait consigner toutes les erreurs ou tous les échecs, avec description et horodatage, lors de la conversion simple ou en lots de documents sources originaux, sources mis à jour et cibles finaux en texte.
CAT-TM-05.26	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de générer des rapports sur toutes les erreurs ou tous les échecs lors de la conversion simple ou en lots de documents sources originaux, sources mis à jour et cibles finaux en texte.
CAT-TM-05.27	***La solution du SGDSL*** devrait permettre la segmentation, l'appariement, l'alignement et le stockage manuel et automatique de textes sources originaux, sources mis à jour et cibles finaux.
CAT-TM-05.28	***La solution du SGDSL*** devrait aviser un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de toutes les erreurs et tous les échecs survenus lors de la segmentation, l'appariement, l'alignement et le stockage de texte.
CAT-TM-05.29	***La solution du SGDSL*** devrait consigner toutes les erreurs ou tous les échecs, avec description et horodatage, survenus lors de la segmentation, de l'appariement, de l'alignement et du stockage de texte.
CAT-TM-05.30	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de générer des rapports sur toutes les erreurs ou tous les échecs survenus lors de la segmentation, de l'appariement, de l'alignement et du stockage de texte.
CAT-TM-05.31	***La solution du SGDSL*** devrait permettre le stockage manuel et automatique des documents sources originaux, sources mis à jour et cibles finaux.
CAT-TM-05.32	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer la période de conservation en stockage pour les documents sources originaux, sources mis à jour et cibles finaux.
CAT-TM-05.33	***La solution du SGDSL*** devrait permettre l'accès simultané à une même mémoire de traduction par plusieurs utilisateurs (893 traducteurs) traduisant des parties d'un même document ou de documents étroitement liés.
CAT-TM-05.34	***La solution du SGDSL*** devrait être capable d'importer un fichier TMX bilingue dans une MT avec des paramètres de langue source-cible et cible-source, par exemple, le logiciel devrait être capable d'importer un fichier TMX comprenant des segments en anglais canadien et en français canadien à la fois dans une MT en anglais-français canadiens et dans une MT en français-anglais canadiens.
CAT-TM-05.35	***La solution du SGDSL*** devrait être capable d'importer un fichier TMX multilingue dans une MT bilingue avec des paramètres de langue visant toutes paires de langues pertinentes, par

SECTION DE L'EDT	Exigence (COTÉE)
	exemple, le logiciel devrait être capable d'importer un fichier TMX comprenant des segments en anglais canadien et en français canadien à la fois dans une MT en anglais-français canadiens et dans une MT en français-anglais canadiens.
Traduction automatique ***La solution du SGDSL*** devrait comporter les fonctionnalités de traduction automatique suivantes :	
CAT-MT-06.1	***La solution du SGDSL*** devrait fournir des IPA (interfaces de programmation d'applications) pour les outils de traduction automatique tiers.
Bases de données terminologiques ***La solution du SGDSL*** devrait comporter les fonctionnalités de base de données terminologiques suivantes :	
CAT-TRMB-07.1	***La solution du SGDSL*** devrait permettre aux utilisateurs de personnaliser les recherches dans la base de données terminologiques en utilisant des expressions courantes.
CAT-TRMB-07.2	***La solution du SGDSL*** devrait être doté des capacités suivantes : a) recherche et remplacement; b) suppression; c) annulation des modifications; d) tri; e) fusion; f) suggestion automatique; g) retrait des éléments en double des bases de données terminologiques.
CAT-TRMB-07.3	***La solution du SGDSL*** devrait permettre la gestion de la terminologie multilingue.
CAT-TRMB-07.4	***La solution du SGDSL*** devrait permettre l'extraction de termes bilingues.
CAT-TRMB-07.5	***La solution du SGDSL*** devrait avoir une fonction d'extraction automatique des termes.
CAT-TRMB-07.6	***La solution du SGDSL*** devrait permettre des recherches simultanées dans de multiples bases de données terminologiques.
CAT-TRMB-07.7	***La solution du SGDSL*** devrait permettre la vérification de termes selon des ensembles de termes prédéfinis.
CAT-TRMB-07.8	***La solution du SGDSL*** devrait permettre l'établissement à distance de bases de termes synchronisées hors ligne par ***projet***.
CAT-TRMB-07.9	***La solution du SGDSL*** devrait permettre l'importation et l'exportation de différents types de bases de données terminologiques comme de la terminologie, des dictionnaires, des glossaires et des lexiques dans divers formats : a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) XML; e) CSV.
CAT-TRMB-07.10	***La solution du SGDSL*** devrait fournir des IPA pour les bases de données terminologiques tierces.
Assurance de la qualité (AQ) ***La solution du SGDSL*** devrait comporter les fonctionnalités d'assurance de la qualité suivantes :	
CAT-QA-08.1	***La solution du SGDSL*** devrait évaluer les éléments suivants : a) les incohérences dans les chiffres; b) la terminologie manquante; c) les erreurs d'orthographe; d) la grammaire;

SECTION DE L'EDT	Exigence (COTÉE)
	e) les traductions incomplètes; f) les traductions vides; g) les répétitions de mots; h) les espaces doubles; i) la ponctuation; j) les majuscules; k) la terminologie en fonction d'un ensemble prédéfini de termes; l) segment par segment; m) la gestion et validation du marquage.
CAT-QA-08.2	***La solution du SGDSL*** devrait fournir des notifications pour les travaux soumis qui contiennent des erreurs non corrigées.
CAT-QA-08.3	***La solution du SGDSL*** devrait permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de personnaliser les vérifications d'AQ à l'aide d'expressions courantes.
CAT-QA-08.4	***La solution du SGDSL*** devrait permettre des vérifications d'AQ en temps réel (à la volée) en fonction d'une configuration prédéfinie ou personnalisable.
CAT-QA-08.5	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'activer et de désactiver les tâches d'assurance de la qualité du projet.
CAT-QA-08.6	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de générer les types de rapports d'AQ suivants : a) prédéfinis, b) personnalisables, c) problèmes, d) résumé.
CAT-QA-08.7	***La solution du SGDSL*** devrait permettre la sauvegarde du rapport d'AQ.
CAT-QA-08.8	***La solution du SGDSL*** devrait permettre l'impression du rapport d'AQ.
CAT-QA-08.9	***La solution du SGDSL*** devrait permettre l'exportation du rapport d'AQ dans les formats suivants : a) MS Excel (xls, xslx), b) MS Word (doc, docx), c) PDF, d) XML; e) CSV.
CAT-QA-08.10	***La solution du SGDSL*** devrait fournir des IPA pour les outils d'AQ tiers.
CAT-QA-08.11	***La solution du SGDSL*** devrait être conforme aux modèles suivants : a) modèle LISA QA; b) cadre dynamique d'évaluation de la qualité de TAUS.
CAT-QA-08.12	***La solution du SGDSL*** devrait permettre aux utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de marquer et d'identifier les segments et les documents dans le corpus (MT) qui sont, par exemple : a) mal alignés; b) dont la qualité laisse à désirer*; c) mal alignés et dont la qualité laisse à désirer; d) de nature sensible en fonction du niveau de classification de sécurité qui devrait être retiré de la ***solution du SGDSL***.

SECTION DE L'EDT	Exigence (COTÉE)
	*Dont la qualité laisse à désirer – le segment trouvé dans la MT est mal traduit ou mal formulé, ou comporte une terminologie incorrecte, des erreurs d'orthographe ou des unités de sens manquantes.
CAT-QA-08.13	***La solution du SGDSL*** devrait permettre à des utilisateurs détenant les permissions, les droits d'accès et les rôles appropriés de produire un rapport sur tous les documents et les segments marqués en fonction des catégories susmentionnées.
CAT-QA-08.14	Le rapport devrait notamment indiquer le numéro de demande, le nom de fichier pour chaque segment et/ou document marqué et toutes les métadonnées connexes, et fournir un lien direct vers les segments et/ou les documents.
CAT-QA-08.15	Les segments et/ou documents marqués doivent être ajoutés à une file d'attente à partir de laquelle un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés peut valider, réaligner, remplacer, supprimer et modifier le contenu.
CAT-QA-08.16	***La solution du SGDSL*** devrait être doté d'une fonctionnalité de rapport d'évaluation de la qualité des documents prête à l'emploi.
CAT-QA-08.17	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de créer, de modifier, de supprimer et d'archiver les rapports d'évaluation de la qualité des services offerts par des ressources internes du Bureau de la traduction et des ressources externes.
CAT-QA-08.18	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer les paramètres du rapport d'évaluation de la qualité des documents, notamment la fréquence, les alertes, les notifications, la distribution, les ressources internes du Bureau de la traduction et les ressources externes.
CAT-QA-08.19	***La solution du SGDSL*** devrait pouvoir effectuer des contrôles d'AQ non seulement après la traduction, mais aussi à la volée ou segment par segment.
Exploration du Web ***La solution du SGDSL*** devrait comporter les fonctionnalités d'exploration du Web suivantes :	
CAT- WCRWL-09.1	***La solution du SGDSL*** devrait assurer une capacité d'exploration du Web afin d'extraire et de récupérer tout texte dans les deux langues officielles des sites Web du gouvernement du Canada qui ont déjà été traduits et publiés sur les sites officiels du gouvernement du Canada afin d'alimenter le corpus.
CAT- WCRWL-09.2	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer les paramètres d'exploration du Web.
CAT- WCRWL-09.3	***La solution du SGDSL*** doit aviser un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de toute erreur ou de tout échec dans l'exploration du Web.
CAT- WCRWL-09.4	***La solution du SGDSL*** devrait consigner toutes les erreurs ou tous les échecs, avec description et horodatage, lors de l'exploration du Web.
CAT- WCRWL-09.5	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de générer des rapports sur l'exploration du Web.
CAT- WCRWL-09.6	***La solution du SGDSL*** devrait pouvoir prendre en charge n'importe quelle URL et extraire n'importe quel texte de différentes pages Web dans les deux langues.

3.8 SECTION G – ANALYSES, RAPPORTS ET VÉRIFICATIONS

3.8.1 Objectifs

La section relative aux analyses, aux rapports et aux vérifications des exigences décrit les capacités que doit fournir ***La solution du SGDSL*** afin de s'assurer qu'il existe un processus fondé sur la technologie servant à l'analyse des données et à la présentation de renseignements en matière de traduction, de terminologie et d'interprétation pouvant être communiqués à différentes personnes, notamment aux cadres supérieurs, aux gestionnaires ainsi qu'aux autres utilisateurs et ressources.

Les exigences relatives aux analyses, aux rapports et aux vérifications englobent un grand nombre d'outils, d'applications et de méthodes qui devraient permettre à SPAC de recueillir des données dans ***La solution du SGDSL***, de définir et d'exécuter des requêtes sur les données, de réaliser des vérifications, de préparer des données aux fins d'analyse, de produire des rapports, et de créer des tableaux de bord pour consulter les données aux fins de la présentation des résultats d'analyse, notamment sur les tendances passées et actuelles, les renseignements et les analyses statistiques mis à la disposition des décideurs et des utilisateurs opérationnels (voir *l'Appendice C - Rapports du Bureau de la traduction pour consulter une liste des types de rapports du Bureau de la traduction*).

3.8.2 Exigences

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
ARA-MAN-01	La ***solution du SGDSL*** doit permettre l'analyse des données.
ARA-MAN-01.1	La ***solution du SGDSL*** doit permettre de produire des rapports.
ARA-MAN-01.2	La ***solution du SGDSL*** doit permettre de réaliser des vérifications.

SECTION DE L'EDT	Exigence (COTÉE)
Analyse La ***solution du SGDSL*** devrait comporter des fonctionnalités d'analyse.	
ARA-ANLT-02.1	Les données, les métadonnées et les renseignements d'analyse devraient être disponibles dans les langues officielles du Canada.
ARA-ANLT-02.2	Un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés devrait pouvoir chercher, filtrer, regrouper, consulter et exécuter des analyses à l'aide de paramètres configurables sur : a) toutes les données saisies et définies par les utilisateurs ; b) toutes les données saisies et stockées par le système.
ARA-ANLT-02.3	Permettre l'importation de données, de métadonnées et de renseignements d'analyse dans divers formats de fichier : a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) JSON, e) CSV f) XML.
ARA-ANLT-02.4	Permettre l'exportation de données, de métadonnées et de renseignements d'analyse dans divers formats de fichier : a) MS Excel (xls, xlsx),

SECTION DE L'EDT	Exigence (COTÉE)
	b) MS Word (doc, docx), c) PDF, d) JSON, e) CSV f) XML.
ARA-ANLT-02.5	Permettre le regroupement d'éléments de données et de métadonnées de traduction, de terminologie et d'interprétation selon plusieurs critères, notamment le client du TB, la ressource, le service, le contrat, l'emplacement et l'heure.
ARA-ANLT-02.6	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer les permissions et les droits d'accès d'analyse pour restreindre, par exemple, l'accès, la consultation, la recherche, le filtrage, l'exécution et la distribution de l'information, des métadonnées et des données.
ARA-ANLT-02.7	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'effectuer des recherches et un filtrage de base.
ARA-ANLT-02.8	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'effectuer des recherches et un filtrage avancés.
ARA-ANLT-02.9	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de sauvegarder, d'imprimer et de télécharger des données et des renseignements d'analyse.
ARA-ANLT-02.10	La ***solution du SGDSL*** devrait fournir des IPA pour les outils d'analyse tiers.
Rapports ***La solution du SGDSL*** devrait comporter les fonctionnalités de production de rapports suivantes :	
ARA-RPTG-03.1	Les données, les métadonnées et les renseignements de rapports devraient être disponibles dans les langues officielles du Canada.
ARA-RPTG-03.2	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de rechercher, de filtrer, de regrouper, de consulter et de générer des rapports à l'aide de données et de paramètres configurables, notamment : i. toutes les données saisies et définies par les utilisateurs; ii. toutes les données saisies et stockées par le système.
ARA-RPTG-03.3	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de définir et de générer des rapports, par exemple, des rapports financiers, administratifs, sur la production et sur la productivité.
ARA-RPTG-03.4	Générer des rapports de flux de travaux de bout en bout configurables pour la traduction, la terminologie et l'interprétation qui reflètent les tâches et les activités pour toute période donnée, par exemple, en temps réel, quotidien, hebdomadaire et mensuel.
ARA-RPTG-03.5	Générer des rapports configurables pour la traduction, la terminologie et l'interprétation qui reflètent la charge de travail pour toute période donnée, par exemple, des rapports en temps réel, quotidiens, hebdomadaires, mensuels et annuels.
ARA-RPTG-03.6	Générer des rapports sur le rendement basés sur des paramètres configurables, par exemple, sur le matériel, le système d'exploitation et les applications Web.
ARA-RPTG-03.7	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de restreindre l'accès, la visualisation, la génération de rapports et la distribution.

SECTION DE L'EDT	Exigence (COTÉE)
ARA-RPTG-03.8	Générer des rapports prédéfinis (prêts à l'emploi) à la fois manuellement et automatiquement en fonction des informations et des données saisies dans le système.
ARA-RPTG-03.9	Générer des rapports spéciaux configurables à la fois manuellement et automatiquement en fonction des informations et des données saisies dans le système.
ARA-RPTG-03.10	Générer des rapports fondés sur les exceptions en fonction de filtres, d'éléments de données et de paramètres.
ARA-RPTG-03.11	Générer des rapports manuellement ou automatiquement pour toute période donnée, par exemple, en temps réel, quotidien, hebdomadaire, mensuel et annuel, par un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés.
ARA-RPTG-03.12	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'exporter des informations et des données de rapport prédéfinies (prêtes à l'emploi) dans divers formats de fichiers : a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) JSON, e) CSV f) XML.
ARA-RPTG-03.13	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'exporter des informations et des données de rapports ponctuels configurables dans divers formats de fichiers : a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) JSON, e) CSV f) XML.
ARA-RPTG-03.14	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de créer et de configurer le format des informations et des données : a) en tableaux; b) en colonnes; c) en tableaux croisés ou en tableaux croisés dynamiques; d) en bandes.
ARA-RPTG-03.15	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de transmettre les rapports manuellement et automatiquement à des moments prédéfinis.
ARA-RPTG-03.16	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de transmettre des rapports individuellement et en utilisant une liste de distribution à des moments prédéfinis.
ARA-RPTG-03.17	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de sauvegarder, d'imprimer et de télécharger des données et des renseignements de rapports.
ARA-RPTG-03.18	***La solution du SGDSL*** devrait fournir des IPA pour les outils de production de rapports tiers.

SECTION DE L'EDT	Exigence (COTÉE)
Vérifications ***La solution du SGDSL*** devrait fournir les capacités de vérification suivantes :	
ARA-ADT-04.1	***La solution du SGDSL*** doit avoir des fonctionnalités de vérification pour saisir en temps réel tous les changements dans le système.
ARA-ADT-04.2	***La solution du SGDSL*** doit avoir des fonctionnalités de vérification pour conserver l'historique de vérification de tout changement dans le système pour une période de temps configurable.
ARA-ADT-04.3	***La solution du SGDSL*** doit saisir tous les changements dans le système en indiquant l'identificateur ou le nom d'utilisateur et l'horodatage ainsi qu'une description du changement.
ARA-ADT-04.4	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de rechercher, de filtrer, de regrouper, de visualiser et d'exécuter une vérification à l'aide de données et de paramètres configurables sur : a) toutes les données saisies et définies par les utilisateurs; b) toutes les données saisies et stockées par la solution.
ARA-ADT-04.5	Les renseignements, les métadonnées et les données de vérification devraient être disponibles dans les langues officielles du Canada.
ARA-ADT-04.6	***La solution du SGDSL*** devrait permettre d'importer des informations et des données de vérifications dans divers formats : a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) Txt, e) Csv.
ARA-ADT-04.7	***La solution du SGDSL*** devrait permettre d'exporter des informations et des données de vérifications dans divers formats : a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) Txt, e) Csv.
ARA-ADT-04.8	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de restreindre l'accès, la visualisation, la génération de vérifications et la distribution.
ARA-ADT-04.9	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de sauvegarder, d'imprimer et de télécharger des données et des renseignements de vérifications.
ARA-ADT-04.10	***La solution du SGDSL*** devrait fournir des IPA pour les outils de vérification tiers.
Tableau de bord La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes :	
ARA-DASH-05.1	Les données et les renseignements du tableau de bord devraient être disponibles dans les langues officielles du Canada.
ARA-DASH-05.2	Un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés devrait pouvoir chercher, filtrer, regrouper, consulter et générer le tableau de bord à l'aide de données et de paramètres configurables sur :

SECTION DE L'EDT	Exigence (COTÉE)
	a) toutes les données saisies et définies par les utilisateurs; b) toutes les données saisies et stockées par le système.
ARA-DASH-05.3	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de glisser-déplacer des données pour visualiser les données d'analyse.
ARA-DASH-05.4	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de choisir parmi une vaste gamme de graphiques et de tableaux pour afficher l'information et les données.
ARA-DASH-05.5	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer les droits d'accès et les permissions du tableau de bord pour restreindre l'accès, la visualisation, la génération du tableau de bord et la diffusion.
ARA-DASH-05.6	Personnaliser le contenu des tableaux de bord intégrés.
ARA-DASH-05.7	Suggérer automatiquement des graphiques et des tableaux en fonction de l'information et des données.
ARA-DASH-05.8	Personnaliser la mise en page et l'affichage de l'information et des données.
ARA-DASH-05.9	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de sauvegarder, d'imprimer et de télécharger des données et des renseignements du tableau de bord.
ARA-DASH-05.10	***La solution du SGDSL*** devrait fournir des IPA pour les outils de tableaux de bord tiers.
Veille économique La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes :	
ARA-BI-06.1	Fournir, habiliter et soutenir une capacité intégrée d'entrepôt de données et de traitement analytique en ligne pour la veille économique et l'établissement de rapports, à l'appui des activités d'analyse telles que le regroupement (fusion), l'analyse descendante et le morcellement des données.

3.9 SECTION H – GESTION DES DONNÉES ET DE L'INFORMATION

3.9.1 Objectif

L'objectif de la présente section est de décrire les exigences relatives à la gestion des données et de l'information qui s'appliquent à l'entrepreneur dans la portée globale de la ***solution du SGDSL*** pour veiller à ce que :

a) les besoins en matière d'information sont comblés selon différents points de vue : politiques, processus et règlements du Bureau de la traduction de SPAC du GC, clients des ministères et des organismes du GC, intervenants et partenaires;

b) l'information respecte des normes de qualité élevées et conserve sa valeur opérationnelle pendant sa durée de vie;

c) l'information circule facilement entre différents systèmes et différentes bases de données;

d) les données de base évoluent constamment au moyen de processus manuels et automatisés;

e) les besoins de données sont protégés contre les défaillances des systèmes et les mécanismes de récupération sont convenus, prévus et mis en œuvre;

f) des possibilités d'agrandissement de l'architecture des bases de données existent pour s'adapter aux modifications apportées aux règlements et aux besoins opérationnels, ainsi que pour permettre des modifications manuelles d'intégrité des données, si nécessaire.

3.9.2 Exigences

Section de l'EDT	Exigence (COTÉE)
Gestion des opérations de la base de données La ***solution du SGDSL*** devrait offrir les fonctionnalités suivantes :	
DTA-DBOP-01.1	Permettre la création et l'échange de formats de fichiers ouverts comprenant des ensembles de données tels que CSV, XML et JSON.
DTA-DBOP-01.2	Importer les données directement à partir d'une source externe en utilisant des formats de fichiers standards tels que CSV, XLS, XLSX, TXT et JSON.
DTA-DBOP-01.3	Exporter les données vers une source externe en utilisant des formats de fichiers standards tels que CSV, XML, XLS, XLSX, TXT et JSON.
DTA-DBOP-01.4	Configurer et gérer les processus d'importation et d'exportation habituels (prévus) et spéciaux en utilisant un ensemble configurable de critères de recherche, de champs, de formats de données, d'options de regroupement et de tri.
DTA-DBOP-01.5	Configurer, prévoir et suivre les opérations suivantes liées aux données : a) l'extraction (exportation); b) la création d'ensembles de données (données ouvertes); c) l'alimentation de bases de données ciblées (base de données de traitement de transactions en ligne, traitement analytique en ligne, architecture orientée services); d) la publication en ligne (c.-à-d. html/RSS-xml); e) des rapports et des requêtes liés aux systèmes et aux utilisateurs.
Gestion des documents, des dossiers et du contenu La ***solution du SGDSL*** devrait offrir les fonctionnalités suivantes :	
DTA-INFM-02.1	Créer et gérer les modèles de documents qui comprennent des listes de vérification, des formulaires et des feuilles de calcul pouvant contenir du texte, des caractéristiques liées au format et des éléments d'un formulaire à remplir, tels que les zones de saisie de texte, les cases, les menus déroulants, les tables de données et les tableaux.
DTA-INFM-02.2	Créer de nouveaux documents à l'aide de différents mécanismes, tels que : i. l'utilisation d'un modèle vierge ou prédéfini; ii. l'importation (téléchargement) d'un document existant; iii. le clonage d'un document existant pour en créer un nouveau.
DTA-INFM-02.3	Saisir les métadonnées pendant la création du document.
DTA-INFM-02.4	La gestion de documents peut ajouter, modifier et supprimer.
Gestion et taxonomie des métadonnées La ***solution du SGDSL*** devrait offrir les fonctionnalités suivantes :	
DTA-META-03.1	Permettre l'importation et l'exportation des termes et de la structure de la taxonomie en utilisant des formats standards comme CSV, XML et TXT.
DTA-META-03.2	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de définir des règles sur la façon dont les métadonnées sont saisies pour

Section de l'EDT	Exigence (COTÉE)
	chaque instance d'un document (p. ex. saisie manuelle, alimentation par menu déroulant à partir de taxonomies ou de contenu de base de données et remplissage automatique).
Archivage de données La ***solution du SGDSL*** devrait permettre l'archivage des données de fichiers.	
DTA-ARCH-04.1	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer des données de fichiers des archives.
DTA-ARCH-04.2	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de définir les règles d'archivage des données de fichiers.
DTA-ARCH-04.3	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de définir, de personnaliser et de configurer les métadonnées des données de fichiers à archiver.
DTA-ARCH-04.4	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de sélectionner le type de données de fichiers à archiver.
DTA-ARCH-04.5	***La solution du SGDSL*** devrait permettre l'archivage automatique des données de fichiers en fonction d'une heure configurable.
DTA-ARCH-04.6	***La solution du SGDSL*** devrait permettre l'archivage manuel des données de fichiers.
DTA-ARCH-04.7	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de récupérer et d'accéder à des données de fichiers archivées.
DTA-ARCH-04.8	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer la période de conservation des données de fichiers.
DTA-ARCH-04.9	***La solution du SGDSL*** devrait assurer le suivi de l'ajout, de la modification et de la suppression de données de fichiers en indiquant l'identificateur ou le nom d'utilisateur, l'horodatage ainsi qu'une brève description.
DTA-ARCH-04.10	***La solution du SGDSL*** devrait permettre les recherches et les interrogations de données de fichiers dans les archives en fonction de filtres standards et personnalisés.
DTA-ARCH-04.11	***La solution du SGDSL*** devrait permettre de générer des rapports standards et personnalisés à partir des archives.
DTA-ARCH-04.12	***La solution du SGDSL*** devrait permettre l'importation et l'exportation des rapports dans divers formats.
DTA-ARCH-04.13	***La solution du SGDSL*** devrait afficher des notifications, des alertes ou des messages d'erreur à un utilisateur si des problèmes sont survenus pendant le processus d'archivage.
DTA-ARCH-04.14	Les messages, les alertes et les notifications d'erreur du SGDSL devraient être consignés dans un journal avec le contenu des messages, des alertes et des notifications du système ainsi que l'horodatage.
DTA-ARCH-04.15	***La solution du SGDSL*** devrait permettre le chiffrement des données de fichiers archivées.
DTA-ARCH-04.16	***La solution du SGDSL*** devrait permettre de comprimer les données de fichiers archivées.
DTA-ARCH-04.17	***La solution du SGDSL*** devrait permettre l'utilisation de scripts pour nettoyer manuellement et automatiquement les données de fichiers des archives en fonction de règles standards et personnalisées ainsi que de filtres.

3.10 SECTION I – GESTION DES UTILISATEURS

3.10.1 Objectif

L'objectif de la présente section consiste à décrire les exigences que doit respecter l'entrepreneur afin de permettre à SPAC de gérer les utilisateurs.

3.10.2 Exigences en matière de gestion des utilisateurs et produits livrables

La présente section fait état des exigences liées aux rôles ou aux groupes, à l'enregistrement, aux profils ou aux comptes, à l'ouverture de session ainsi qu'aux justificatifs.

3.10.3 Exigences

SECTION DE L'EDT	Exigence (Obligatoire)
USR-ROLE-1.0	**Rôles / groupes** La ***solution du SGDSL*** doit fournir la capacité de gérer les rôles et les groupes d'utilisateurs.
USR-REG-2.0	**Enregistrement** La ***solution du SGDSL*** doit avoir la capacité d'enregistrement des utilisateurs.
USR-ACCT-3.0	**Profils / comptes** La ***solution du SGDSL*** doit permettre la gestion des profils d'utilisateurs et des comptes.
USR-LOGN-4.0	**Ouverture de session** La ***solution du SGDSL*** doit authentifier un utilisateur au moment de l'ouverture de session.
USR-CRED-5.0	**Justificatifs** La ***solution du SGDSL*** doit permettre à un utilisateur d'utiliser les informations d'identification.

SECTION DE L'EDT	Exigence (COTÉE)
Rôles/groupe La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes :	
USR-ROLE-01.1	Fournir un contrôle d'accès basé sur les rôles qui définit les droits d'accès et les autorisations, les caractéristiques et les fonctionnalités de la solution.
USR-ROLE-01.2	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de définir et d'administrer les types d'utilisateurs, les rôles et les groupes.
USR-ROLE-01.3	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'assigner des utilisateurs à des groupes.
USR-ROLE-01.4	Permettre la définition d'une variété de groupes, de rôles et de types d'utilisateurs.
USR-ROLE-01.5	Permettre à un seul utilisateur d'avoir plusieurs rôles.

SECTION DE L'EDT	Exigence (COTÉE)
USR-ROLE-01.6	Restreindre l'accès des utilisateurs afin de leur permettre d'accéder uniquement aux informations, aux métadonnées et aux données correspondant à leurs rôles, leurs groupes et leurs types d'utilisateurs.
USR-ROLE-01.7	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer des groupes d'utilisateurs.
USR-ROLE-01.8	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer des utilisateurs dans un ou plusieurs groupes d'utilisateurs.
USR-ROLE-01.9	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer les droits d'accès aux caractéristiques et aux fonctionnalités d'un utilisateur individuel au niveau du groupe.
USR-ROLE-01.10	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'examiner, de valider, d'ajouter, de modifier et de supprimer les caractéristiques d'un profil d'utilisateur.
USR-ROLE-01.11	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'examiner, de valider, d'ajouter, de modifier et de supprimer les caractéristiques et les paramètres d'un utilisateur dans des groupes.
USR-ROLE-01.12	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de déléguer son propre rôle à un autre utilisateur pour une période de temps configurable.
Enregistrement ***La solution du SGDSL*** devrait comporter les fonctionnalités suivantes :	
USR-REG-02.1	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'inscrire un utilisateur.
USR-REG-02.2	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de s'inscrire.
USR-REG-02.3	Pour valider les informations d'enregistrement de l'utilisateur
Profils/ Comptes L'entrepreneur doit livrer une solution qui comporte les fonctionnalités suivantes :	
USR-ACCT-03.1	Créer et gérer des informations de profil d'utilisateur configurables qui peuvent être utilisées comme attributs dans la solution, par exemple : région, langue de préférence, fuseau horaire, coordonnées, nom du gestionnaire et cote de sécurité.
USR-ACCT-03.2	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier, de supprimer, de désactiver et de fermer des profils d'utilisateurs individuels dans la ***solution du SGDSL***.
USR-ACCT-03.3	Conserver les dossiers et les renseignements sur les comptes d'utilisateur dans la ***solution du SGDSL*** pour qu'un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés puisse y accéder pendant une période de temps configurable.
USR-ACCT-03.4	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de cloner des profils d'utilisateurs pour de nouveaux utilisateurs.
USR-ACCT-03.5	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de cloner des profils d'utilisateurs et de modifier les paramètres et les éléments spécifiques des profils.

SECTION DE L'EDT	Exigence (COTÉE)
USR-ACCT-03.6	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de gérer les comptes d'utilisateurs une fois qu'ils sont créés, par exemple, en envoyant des notifications à l'utilisateur concernant l'utilisation du compte, et de mettre à jour les informations sur le compte.
USR-ACCT-03.7	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés d'ajouter, de modifier et de supprimer des comptes d'utilisateurs au nom des utilisateurs.
USR-ACCT-03.8	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de rechercher, d'afficher, d'ajouter, de modifier et de supprimer des changements dans le profil de n'importe quel utilisateur.
USR-ACCT-03.9	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de rechercher, d'afficher, d'ajouter, de modifier et de supprimer des changements dans le compte de n'importe quel utilisateur.
Ouverture de session La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	
USR-LOGN-04.1	Exiger qu'un utilisateur s'authentifie lorsqu'il accède à la ***solution du SGDSL*** et à tout autre composant applicable à l'aide d'un nom d'utilisateur et d'un mot de passe.
USR-LOGN-04.2	Permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de mettre sur pied une authentification à facteurs multiples.
USR-LOGN-04.3	***La solution du SGDSL*** devrait permettre à un utilisateur de changer et de réinitialiser le mot de passe.
USR-LOGN-04.4	***La solution du SGDSL*** devrait demander à l'utilisateur d'entrer l'ancien et le nouveau mot de passe lorsqu'il change ou réinitialise le mot de passe.
USR-LOGN-04.5	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer le nombre des caractères du mot de passe et les règles connexes.
USR-LOGN-04.6	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de configurer le nombre de réutilisations du mot de passe.
USR-LOGN-04.7	***La solution du SGDSL*** devrait permettre d'effectuer le suivi des tentatives de connexion d'un utilisateur.
USR-LOGN-04.8	***La solution du SGDSL*** devrait être capable de verrouiller un utilisateur après plusieurs tentatives de connexion infructueuses.
USR-LOGN-04.9	***La solution du SGDSL*** devrait permettre à un utilisateur détenant les permissions, les droits d'accès et les rôles appropriés de définir le nombre d'échecs de tentatives de connexion.
USR-LOGN-04.10	***La solution du SGDSL*** devrait pouvoir chiffrer le nom d'utilisateur et le mot de passe lorsque l'utilisateur a soumis les justificatifs pour l'authentification.
USR-LOGN-04.11	Masquer le mot de passe entré par l'utilisateur.
Justificatifs La ***solution du SGDSL*** devrait comporter les fonctionnalités suivantes.	

SECTION DE L'EDT	Exigence (COTÉE)
USR-CRED-05.1	Pour transférer ou télécharger directement les justificatifs d'identité des utilisateurs autorisés vers la ***solution du SGDSL*** et tout autre composant applicable.
USR-CRED-05.2	Fournir la capacité de définir les informations d'identification des utilisateurs autorisés à la ***solution du SGDSL*** et à tout autre composant applicable.

4 EXIGENCES TECHNIQUES

4.1 TECHNOLOGIE DE L'INFORMATION, ET MAINTENANCE ET MISE À JOUR DE LA SOLUTION

4.1.1 Solution hébergée – SGDSL

L'entrepreneur doit fournir, configurer, mettre à l'essai, mettre en œuvre, prendre en charge et gérer, dans les deux langues officielles du Canada, une ***solution de SGDSL,*** y compris le matériel de technologie de l'information et les composantes logicielles pertinentes ainsi que les processus opérationnels connexes, afin de répondre aux exigences fonctionnelles décrites dans l'Énoncé des travaux.

Le SGDSL doit permettre les modifications, les rajustements ou les ajouts de flux de travaux de processus opérationnel, de fonctions automatisées de système, et d'autres processus et règles de gestion linguistique connexes, sans qu'il faille modifier le code de l'application.

Les composantes du SGDSL doivent comprendre une fonction permettant l'intégration avec les composantes de technologie de l'information utilisées par le GC et les partenaires de prestation.

Le SGDSL doit comprendre le soutien à la gestion et aux opérations de l'infrastructure informatique et réseau sur demande, qui est souple, évolutive et solide.

4.2 EXIGENCES RELATIVES AU MATÉRIEL

SPAC cherche à acquérir une ***solution de SGDSL*** en tant que service géré par l'entrepreneur, qui utilise les applications du fournisseur hébergées sur l'infrastructure de l'entrepreneur ou du sous-traitant.

L'entrepreneur doit élaborer, configurer, mettre à l'essai, mettre en œuvre, prendre en charge, tenir à jour et héberger toute l'infrastructure à l'appui de la solution visant à répondre à l'ensemble des exigences définies dans l'Énoncé des travaux.

4.3 INTEROPÉRABILITÉ AVEC LES AUTRES SYSTÈMES ET ENVIRONNEMENTS

4.3.1 Contexte

Afin de développer et de soutenir des services linguistiques rationalisés, la ***solution du SGDSL*** peut nécessiter l'échange d'informations et de données avec d'autres systèmes et environnements.

Cette section décrit les exigences en matière d'échange de données pour le SGDSL et les exigences techniques connexes en fonction de l'information actuelle :

a) garantir que le SGDSL est harmonisé avec les normes de SPAC et qu'il favorise l'interopérabilité avec les processus, les données, les systèmes et les environnements de SPAC et d'autres entités;
b) déterminer et préciser les besoins d'échange de données de haut niveau avec d'autres systèmes ministériels et d'autres sources de données non-SPAC.

Les exigences figurant à la section 4,4, *Exigences technologiques du SGDSL*, concernent les normes, les politiques, les directives et les exigences applicables en matière de technologie à l'appui des exigences d'échange de données indiquées dans la présente section.

4.3.2 Interopérabilité générale du système

Il est nécessaire de disposer d'interfaces externes structurées et modulaires qui permettront l'échange d'informations et de données entre la ***solution du SGDSL*** et d'autres systèmes et environnements au moyen d'une infrastructure sécurisée.

Les interfaces peuvent comprendre :

a) un intranet ou un extranet;
b) les services Web tels que les flux de données de tiers;
c) des composantes de sécurité commerciales d'une tierce partie;
d) d'autres systèmes contenant de l'information et des données qui sont saisies pour être utilisées dans la ***solution du SGDSL***;
e) Adaptateurs ou connecteurs génériques disponibles sur le marché pour l'interface avec d'autres systèmes et environnements tels que SIGMA.

L'entrepreneur doit fournir une liste de toutes les interfaces touchées et des modules d'interopérabilité des applications de tiers et/ou des interfaces de programmation d'applications (API) utilisées dans la solution.

L'entrepreneur doit s'assurer que ces API sont compatibles avec les systèmes de SPAC.

À l'appui des plans stratégiques de SPAC pour l'interopérabilité des applications, la ***solution du SGDSL*** doit exposer sa fonctionnalité au moyen d'une API qui tire parti des protocoles API standard de l'industrie.

L'entrepreneur doit fournir une trousse d'outils d'intégration des applications que d'autres fournisseurs de solutions peuvent utiliser pour créer des méthodologies d'intégration, tel que demandé par SPAC, pour leurs applications, y compris :

a) outil d'intégration des applications d'entreprise qui respecte le support et le format précisés par SPAC;
b) documents de référence (en anglais canadien et en français canadien) sur l'utilisation de l'outil, notamment ce qui suit :
c) manuels et guides du fabricant d'équipement d'origine;
d) documents d'instructions donnant des détails sur les mesures de contrôle, les méthodes, les dictionnaires de données, etc.;
e) pratiques exemplaires et livres blancs;
f) exemple de code source pour l'intégration des applications;
g) liste de toutes les bibliothèques prises en charge par le SGDSL;
h) guide d'essai de conformité des applications qui comprend ce qui suit :
    i. scénarios d'essai que les partenaires de SPAC peuvent utiliser pour évaluer la conformité d'une application aux protocoles et aux normes pris en charge;

ii. liste de vérification de la conformité que les partenaires de SPAC peuvent remplir pour consigner les résultats des essais de conformité et en faire rapport.

4.3.3 Interopérabilité technique

À l'appui des plans stratégiques de SPAC pour l'interopérabilité des applications, la ***solution du SGDSL*** doit exposer sa fonctionnalité au moyen d'une API qui tire parti des technologies et protocoles API standard de l'industrie.

La ***solution du SGDSL*** doit interagir avec la suite informatique de SPAC, par exemple l'infrastructure et la plate-forme telles que déterminées et demandées par SPAC sans modification importante de l'infrastructure actuelle de SPAC ou changements aux ordinateurs de bureau.

4.3.4 Exigences

SECTION DE L'EDT	Exigence (COTÉE)
La ***solution du SGDSL*** doit comporter les fonctions d'interface suivantes :	
TEC-INTFC-01	Créer et envoyer des renseignements aux ressources à partir du SGDSL, par l'intermédiaire d'avis (courriel ou alertes sur le portail).
TEC-INTFC-02	Permettre les échanges de données en direction et en provenance des systèmes en place pendant la période de transition en utilisant la fréquence, les styles et les méthodes d'interface privilégiés par SPAC : a) temps réel ou lots; b) services Web ou API; c) langage XML ou fichier non hiérarchique.
TEC-INTG-02	Permettre l'échange de données avec SIGMA au moyen des mécanismes d'interface spécifiés par SIGMA plutôt que par appels d'API en raison des restrictions concernant le zonage du réseau SIGMA.
TEC-INTG-02.1	La solution doit permettre l'intégration future à divers autres systèmes et environnements qui seront déterminés par le **client** en collaboration avec l'entrepreneur.
TEC-INTG-03	La solution doit gérer correctement l'encodage des jeux de caractères pour les fichiers texte importés vers le SGDSL ou exportés à partir du SGDSL**.**
TEC-INTG-03.1	Les fichiers texte, les fichiers XML ou les fichiers basés sur le langage XML générés par le SGDSL seront encodés dans le format UTF-8, à moins d'avis contraire du Canada.
TEC-INTG-03.2	Les fichiers XML et les fichiers de téléchargement basés sur le langage XML acceptés par le SGDSL seront encodés dans le format UTF-8 ou dans un autre format précisé dans l'étiquette d'en-tête de fichier, à moins d'avis contraire du Canada.

SECTION DE L'EDT	Exigence (COTÉE)
TEC-INTG-03.3	Tout volet du SGDSL qui accepte le téléchargement de fichiers texte permettra également d'identifier le format d'encodage des caractères du fichier (p. ex., UTF-8, UTF-16, ISO-8859-1, etc.), à moins d'avis contraire du Canada.

4.4 EXIGENCES TECHNOLOGIQUES DU SGDSL

4.4.1 Introduction

Le SGDSL doit être une solution souple, adaptable et évolutive qui répond aux besoins opérationnels changeants, principalement par la gestion des configurations offertes dans la solution.

Les exigences de cette section décrivent ce que la solution doit fournir, permettre et soutenir en termes de capacités techniques qui doivent être satisfaites pour que la solution coexiste et interopérable.

Les versions et les applications, systèmes et outils du GC ou de SPAC seront fournis lorsqu'ils seront connus. Comme c'est le cas pour toutes les autres politiques et normes du GC, les normes technologiques évoluent, et l'on s'attend à ce que le SGDSL prenne en charge les changements de normes technologiques demandés par SPAC.

4.4.2 Conformité

Les exigences de conformité de la ***solution du SGDSL*** sont définies dans la *Partie 2, Exigences relatives aux lois, aux règlements et aux politiques*.
Les exigences présentées dans cette section constituent des exigences de conformité propres aux technologies du SGDSL qui doivent faciliter la conformité de SPAC aux politiques, aux directives et aux lignes directrices énoncées.

4.4.3 Interopérabilité

La ***solution du SGDSL*** doit pouvoir, au besoin, être compatible avec les applications, les systèmes et les outils de SPAC, de l'entrepreneur et des tiers, par exemple, en employant à tout le moins les éléments suivants :

a) les API (prêtes à l'emploi, ou développées en partie ou en totalité);
a) l'importation et l'exportation des données et du contenu de la ***solution du SGDSL***.

4.4.4 Convivialité

La convivialité est la facilité d'utilisation et d'apprentissage du SGDSL. Les exigences de convivialité de cette section se concentrent sur les meilleures pratiques et normes de SPAC et de l'industrie des TI qui ont été largement adoptées pour la création et la maintenance d'applications Web faciles à utiliser.

4.4.5 Fiabilité

Les exigences de cette section précisent les capacités et l'architecture de la solution qui, en général, offrent un niveau de disponibilité plus élevé, des applications plus faciles à maintenir et une plus grande résilience globale.

4.4.6 Adaptabilité

L'adaptabilité devrait faire partie de la *solution du SGDSL* en étant en mesure de faire face à une augmentation de volume sur demande sans impact sur le rendement.

4.4.7 Exigences

SECTION DE L'EDT	Exigence (COTÉE)
La ***solution SGDSL*** devrait comporter les fonctionnalités suivantes :	
TECH-01.1	Être compatible avec les applications, les systèmes et les outils du GC, de SPAC, de l'entrepreneur et des tiers en employant les éléments suivants : a) les API (prêtes à l'emploi, ou développées en partie ou en totalité); b) l'importation et l'exportation des données et du contenu de la ***solution du SGDSL***.
TECH-01.2	Appuyer le concept d'architecture ouverte et donner l'accès à ses services, à ses caractéristiques et à ses fonctionnalités au moyen d'autres API, services Web et technologies similaires fournis par des entrepreneurs ou des tiers.
TECH-01.3	Prendre en charge les pages Web et les fils de nouvelles Web encodés selon le format UTF-8 et UTF-16 (Unicode Transformation Format).
TECH-01.4	Permettre l'interopérabilité en temps réel au moyen d'une architecture de services Web, p. ex., REST (HTTPS, encodage JSON ou XML) et SOAP (HTTPS ou JMS).
TECH-01.5	Permettre l'adaptabilité verticale des ressources physiques pour gérer la charge et l'augmentation de volume sur demande sans redémarrage et sans que cela nuise au rendement.
TECH-01.6	Comprendre un dispositif d'équilibrage de la charge pour contrôler et distribuer le trafic d'entrée.
TECH-01.7	Pour favoriser le rendement et l'adaptabilité du serveur d'applications et du serveur Web, la fonction de réglage devrait comprendre ce qui suit : a) intégration de l'adaptabilité : i. une fonction intégrée; ii. une capacité externe. b) fonction de réglage du rendement incluant ce qui suit, sans s'y limiter : i. équilibrage de charge dynamique; ii mise en grappe; iii. mise en cache de composantes de l'environnement d'applications afin d'accroître le rendement.
TECH-01.8	Fournir des environnements de simulation distincts, au besoin, aux fins de configuration, de mise à l'essai et de formation pour les nouvelles versions de logiciels.
TECH-01.9	Permettre le versionnage des configurations, et le redéploiement des versions de production antérieures.

SECTION DE L'EDT	Exigence (COTÉE)
TECH-01.10	Permettre l'application de pratiques exemplaires de sécurisation des services Web, comme celles du guide sur les services Web sécurisés (publication spéciale 800-95 du National Institute of Standards and Technology [NIST]).
TECH-01.11	Fermer automatiquement une session Web après un délai d'inactivité, lequel sera fixé par SPAC.
TECH-01.12	Permettre à toute base de données de gérer et de protéger des données pouvant atteindre le niveau Protégé B.
TECH-01.13	Fournir la solution dans un réseau distinct et un environnement réparti en zones de telle sorte que l'infrastructure du SGDSL est divisée en zones selon le niveau de confiance, si bien que : a) la séparation logique des données est préservée; b) la séparation physique est liée par des dispositifs de limite.
TECH-01.14	Respecter la norme actuelle de navigateur Web du GC, soit Microsoft Internet Explorer 11, et prendre en charge deux versions antérieures d'importance à mesure qu'évolue la norme.
TECH-01.15	Assurer la compatibilité avec les autres navigateurs Web, p. ex. Edge, Firefox, Safari et Chrome.
TECH-01.16	Soutenir la capacité de fonctionner comme une solution basée sur un navigateur Web sécurisé qui ne nécessite pas l'installation d'autres logiciels de bureau et modules d'extension (add-on) sur le poste de travail de l'utilisateur en plus d'un navigateur Web.
TECH-01.17	Fournir la capacité permettant à un utilisateur de naviguer directement vers un écran exploitable à partir de la notification demandant une action, sans avoir à ouvrir de nouveau une session.
TECH-01.18	Permettre la validation et la confirmation de la saisie des données selon le type de champ, la taille des données, les propriétés du tableau et la liste des valeurs préconfigurées (p. ex., seul le format de code postal valide sera accepté pour le code postal).
TECH-01.19	Fournir le style d'architecture permettant une bonne gestion des erreurs, la restauration et la notification aux utilisateurs lorsque des erreurs se produisent en ligne.
TECH-01.20	Par souci de convivialité, intégrer les pratiques exemplaires quant aux principes de conception des applications Web W3C, p. ex., boutons d'activation et de désactivation, options et transmission des données fondées sur les valeurs saisies par l'utilisateur, réduction des messages-guides inutiles.
TECH-01.21	Permettre la connexion unique (identification unique – IU) des utilisateurs du GC pour fournir un accès basé sur les rôles à toutes les composantes du SGDSL.
TECH-01.22	Permettre l'utilisation du système d'exploitation actuel du GC, Microsoft Windows 7 Enterprise et les versions plus récentes.

SECTION DE L'EDT	Exigence (COTÉE)
TECH-01.23	Appuyer la capacité de sécuriser les données en transit à l'aide du protocole de transfert hypertexte sécurisé (HTTPS) et du protocole de sécurité de la couche transport (TSL 1.2 ou supérieur), pour répondre aux exigences de chiffrement des données précisées à la section 5.3.9 (Exigences en matière de sécurité – Chiffrement).
TECH-01.24	Les serveurs de la ***solution du SGDSL*** doivent avoir une mémoire non volatile afin que les changements enregistrés sur le disque ne soient pas perdus si l'on éteint ou démarre un serveur dans le cadre d'une activité planifiée ou imprévue.
TECH-01.25	La ***solution du SGDSL*** doit permettre à un utilisateur qui détient les rôles, les droits d'accès et les permissions appropriés de surveiller l'utilisation des ressources physiques du serveur en temps réel.
TECH-01.26	L'hyperviseur de virtualisation assistée par le matériel de la ***solution du SGDSL*** doit être séparé des autres hyperviseurs de virtualisation.
TECH-01.27	La ***solution du SGDSL*** doit permettre la portabilité de la machine virtuelle.
TECH-01.28	La machine virtuelle de la ***solution du SGDSL*** doit faire l'objet d'une sauvegarde.
TECH-01.29	La ***solution du SGDSL*** doit avoir la capacité de ramener une machine virtuelle à un état antérieur.
TECH-01.30	La ***solution du SGDSL*** doit permettre d'identifier les machines virtuelles à l'aide d'étiquettes/de métadonnées.
TECH-01.31	Le temps de disponibilité et le délai de réponse de la ***solution du SGDSL*** doivent être surveillés en temps réel.
TECH-01.32	L'utilisation de la largeur de bande du réseau de la ***solution du SGDSL*** doit être surveillée en temps réel.
TECH-01.33	La ***solution du SGDSL*** doit permettre la surveillance de la base de données, notamment de ce qui suit : a) l'utilisation des entrées-sorties; b) le rendement relatif aux recherches (exécution – succès et erreur); c) le débit de traitement; d) le temps d'attente.
TECH-01.34	La ***solution du SGDSL*** doit pouvoir prendre en charge 2000 utilisateurs simultanés.
TECH-01.35	La ***solution du SGDSL*** doit prévoir des indicateurs de rendement permettant d'évaluer ce qui suit : a) l'application; b) le système d'exploitation; c) la virtualisation; d) le réseau; e) la base de données.
TECH-01.36	La ***solution du SGDSL*** doit permettre à un utilisateur détenant les permissions et les droits d'accès appropriés de consulter les rapports de rendement sur : a) l'application; b) le système d'exploitation; c) la virtualisation;

SECTION DE L'EDT	Exigence (COTÉE)
	d) le réseau; e) la base de données.
TECH-01.37	La ***solution du SGDSL*** doit permettre à un utilisateur détenant les permissions et les droits d'accès appropriés de personnaliser l'affichage des rapports de rendement sur : a) l'application; b) le système d'exploitation; c) la virtualisation; d) le réseau; e) la base de données.
TECH-01.38	La ***solution du SGDSL*** doit permettre à un utilisateur détenant les permissions et les droits d'accès appropriés de générer des rapports de rendement sur : a) l'application; b) le système d'exploitation; c) la virtualisation; d) le réseau; e) la base de données.
TECH-01.39	La ***solution du SGDSL*** doit enregistrer les événements, les dépassements de seuils, les erreurs, les avertissements ainsi que les alertes, et inclure l'identificateur, le type, la marque d'horodatage et la description, pour ce qui suit : a) l'application; b) le système d'exploitation; c) la virtualisation; d) le réseau; e) la base de données.
TECH-01.40	La ***solution du SGDSL*** doit permettre à un utilisateur détenant les permissions et les droits d'accès appropriés de personnaliser les rapports de rendement en fonction de ce qui suit : a) l'application; b) le système d'exploitation; c) la virtualisation; d) le réseau; e) la base de données.
TECH-01.41	L'entrepreneur doit signaler à SPAC les limites en matière d'adaptabilité ou d'accès qui pourraient prendre effet à n'importe quelle étape du contrat ou en ce qui a trait au respect des exigences liées à l'adaptabilité et au rendement.
TECH-01-42	La connexion réseau entre SPAC et la ***solution du SGDSL*** devrait fournir une capacité de connexion de 1 GBit/sec ou plus.

5 EXIGENCES NON FONCTIONNELLES

5.1 CONTEXTE

La présente partie vise à établir les résultats ou exigences qui s'appliquent à l'ensemble des éléments de la **solution SGDSL**.

5.2 ENGAGEMENTS GÉNÉRAUX

5.2.1 Adaptation aux changements

La **solution SGDSL** doit pouvoir être adaptée aux changements au sein de SPAC selon un calendrier convenu. SPAC prévoit que les types de modifications suivantes devront probablement être apportés durant la période du contrat :

a) Modifier un flux de travaux ou en ajouter un nouveau pour tenir compte des nouvelles politiques ou approches des processus du Bureau de la traduction;
b) Modifier un élément de données ou en ajouter un afin de satisfaire à une nouvelle exigence en matière d'établissement de rapports ou d'adapter la solution aux changements apportés aux dictionnaires de données existants;
c) Modifier des messages de communication ou en ajouter de nouveaux;
d) Importer des renseignements de services ou systèmes nouveaux ou existants et/ou exporter des renseignements vers ceux-ci;
e) Modifier des politiques et des exigences administratives;
f) Modifier des connecteurs ou des API ou en ajouter de nouveaux.

SPAC prévoit que les ressources et les activités liées à la modification du SGDSL souple et configurable pourraient entraîner des coûts de gestion du changement. Or, selon les exigences relatives à la capacité de technologie de l'information de l'entrepreneur, établies dans la description donnée à la *Partie 5 : Exigences non fonctionnelles*, celui-ci doit fournir une solution souple qu'on peut adapter au fil du temps sans que les ces modifications entraînent des coûts importants de gestion du changement de la technologie de l'information.

5.2.2 Souplesse de la solution

L'entrepreneur doit être en mesure d'avoir accès au codage de la ***solution SGDSL***, lorsque le responsable technique l'y autorise ou lui ordonne de le faire, pour trouver des solutions de rechange afin de modifier ou de suspendre les opérations courantes. Lorsque l'entrepreneur est appelé à modifier la solution, il doit :

a) consigner les changements apportés au processus;
b) tenir des registres complets de l'incidence du changement;
c) rédiger des rapports ponctuels pour quantifier et qualifier les changements découlant de la modification ou de la suspension des processus.

Adaptation aux changements attribuables aux politiques
Les changements touchant l'environnement, les politiques et les processus sont fréquents. La ***solution SGDSL*** doit être suffisamment souple afin qu'on puisse l'adapter aux changements et modifier les flux de travaux, les zones de données, les processus et les configurations selon les indications du gouvernement du Canada.

5.2.3 Convivialité de la solution

L'entrepreneur doit adopter et mettre à profit des pratiques exemplaires en matière de conception de solutions. Il doit par exemple :

a) garantir que l'interface utilisateur de la **solution du SGDSL** soit uniforme et normalisée;
b) guider les utilisateurs en fournissant des messages d'aide contextuels et des schémas de processus visuels à la demande de SPAC;
c) concevoir une interface d'utilisateur intuitive en suivant les pratiques exemplaires en conception Web, notamment en rendant les objets interactifs évidents, en faisant donnant de la rétroaction, en évitant les répétitions aux utilisateurs et en indiquant toujours les valeurs par défaut dans les champs et les formulaires;
d) par souci de convivialité, intégrer des outils et des plugiciels représentant des pratiques exemplaires en matière de conception des applications Web, comme l'affichage d'information au passage de la souris, le remplissage automatique, un calendrier, une zone de liste déroulante à choix multiples, un sélecteur de date, un gestionnaire glisser-déplacer, des touches de raccourci;
e) veiller à une intégration en douceur avec les outils de productivité et l'environnement bureautique, notamment en offrant la compatibilité « glisser-déplacer » avec la suite logicielle Microsoft Office;
f) permettre aux utilisateurs de créer des hyperliens menant à n'importe quel document pour qu'on puisse y renvoyer n'importe où dans la solution;
g) permettre aux utilisateurs de personnaliser et de gérer leurs propres aperçus, notamment en créant des favoris et des raccourcis et en configurant des actions par défaut ainsi que des valeurs par défaut pour les données et processus opérationnels.

5.2.4 Principes de gestion efficace de l'information

La gestion de l'information fait partie intégrante des responsabilités de l'entrepreneur. Grâce aux indicateurs de rendement clés et aux données transactionnelles, le Bureau de la traduction peut mesurer le rendement et en rendre compte, créer des politiques et maintenir un service à la clientèle de grande qualité, et ce, à toutes les étapes du cycle de vie du projet (demande).

L'entrepreneur doit appliquer les principes de base de gestion de l'information efficace pour :

a) éviter la collecte inutile de données en double, corriger les incohérences et veiller à la qualité des données;
b) veiller à ce que l'information soit complète, exacte, à jour, pertinente et compréhensible;
c) appuyer l'accès à l'information sous réserve des exigences stratégiques et juridiques;
d) empêcher un accès illégal à l'information;
e) protéger l'information des accès non autorisés, des pertes et des dommages.

De plus, l'entrepreneur doit fournir des renseignements à SPAC concernant :

f) les renseignements qui doivent être saisis et utilisés et la façon de le faire;
g) la durée de fonctionnement d'un programme ou d'un service ;
h) le temps pendant lequel on aura besoin des renseignements à des fins opérationnelles, juridiques ou de preuve.

5.3 EXIGENCES EN MATIÈRES DE SÉCURITÉ

5.3.1 Sécurité

L'*Appendice G – Sécurité et protection des renseignements personnels* contient les exigences détaillées en matière de sécurité ainsi que de la matrice de traçabilité des exigences relatives à la sécurité (MTERS).

L'entrepreneur doit veiller à ce que les centres de données, les logiciels, les intergiciels et le bureau de service du SGDSL ainsi que l'infrastructure et les données du Centre des opérations de protection (COP) et du Centre d'exploitation de réseau pour l'ensemble de la ***solution SGDSL*** soient hébergés au Canada.

L'entrepreneur doit veiller à ce que tous les travaux visés par le contrat (y compris le COP, le Centre d'exploitation de réseau et le bureau de service) effectués par le personnel de l'entrepreneur, que ce soit par l'entremise d'un sous-traitant ou d'un autre intervenant, soient effectués au Canada.

L'entrepreneur doit garantir que toute entité commerciale effectuant des travaux prévus au contrat ait un emplacement physique au Canada.

5.3.2 Renseignements personnels

La *Loi sur la protection des renseignements personnels* prévoit des limites quant à la collecte, l'utilisation et la divulgation des renseignements personnels par les institutions du gouvernement fédéral. Elle confère également aux Canadiens le droit de consulter et de corriger les renseignements personnels les concernant qui sont détenus par les institutions.

L'entrepreneur doit protéger tous les renseignements personnels et protégés, notamment :

a) les renseignements sur l'identité des ressources du Bureau de la traduction;
b) les renseignements financiers des ressources du Bureau de la traduction;
c) les procédures, les formulaires, les systèmes informatiques et la disposition des fichiers de données, les sites Internet, etc.;
d) les coordonnées (y compris le nom commercial/de l'entreprise), les données biographiques, les renseignements sur la scolarité, les renseignements financiers, les renseignements sur les habilitations de sécurité, les évaluations, les autres numéros d'identité (p. ex. numéro d'entreprise) et la signature;
e) les documents de traduction (clients) qui contiennent des renseignements personnels.

5.3.3 Renseignements protégés

L'entrepreneur doit:

a) garder en lieu sûr ces renseignements et protéger leur confidentialité et, à la clôture du contrat, les retourner à SPAC;
b) veiller à ce que la conversion, l'imagerie et la destruction subséquente des renseignements personnels contenus dans le contrat soient effectuées conformément aux lois et aux politiques applicables;
c) garder en lieu sûr tous les renseignements créés, détruits, conservés, consultés et modifiés lors de la prestation de la solution conformément aux exigences prescrites par la loi. Ce faisant, la ***solution SGDSL*** doit :

i. comprendre des éléments servant garantir que la qualité, l'exactitude, l'exhaustivité et l'intégrité des données consignées dans la **solution du SGDSL** soient toujours préservées grâce à l'application de mesures de validation pertinentes;
ii. comprendre des éléments servants à garantir que la cohérence des données puisse être vérifiée et que les données puissent être rapprochées;
iii. maintenir un historique par voies multiples des données envoyées ou reçues, des données échangées et des mises à jour de comptes effectuées par le client du BT ou au nom du client du BT;
iv. protéger les renseignements de nature délicate contre le vol, notamment le vol d'identité ou des gestes posés par des tiers non autorisés au nom de clients du BT, la fraude ou la divulgation, conformément à la *Loi sur la protection des renseignements personnels*;
v. comprendre des éléments servant à garantir que toute destruction de dossiers soit effectuée selon les normes prescrites par la *Loi sur la Bibliothèque et les Archives du Canada* et l'Autorisation de disposition du SGDSL.

5.3.4 Programme d'évaluation et d'autorisation de sécurité et conformité en la matière

L'entrepreneur doit participer au programme d'évaluation et d'autorisation de sécurité en ce qui concerne la **solution du SGDSL**. Le programme d'évaluation et d'autorisation de sécurité repose sur le Processus d'application de la sécurité dans les systèmes d'information (PASSI). Pour de plus amples renseignements, voir la *Partie 6 : Processus d'évaluation et d'autorisation de sécurité de SPAC*.

5.3.5 Gestion des risques

L'entrepreneur doit maintenir la posture de sécurité de la solution au moyen d'une surveillance continue et de vérifications annuelles des exigences de sécurité mises en œuvre. Il doit notamment:

a) surveiller les menaces et vulnérabilités;
b) prendre des mesures d'atténuation proactives;
c) signaler au coordonnateur de la sécurité de la TI de SPAC tout problème de sécurité dès qu'il est repéré;
d) faire un suivi de chacun des problèmes de sécurité et présenter des rapports d'étape au coordonnateur de la sécurité de la TI de SPAC et ce, jusqu'à ce que le problème soit réglé ou atténué.

5.3.6 Contrôle d'accès

L'entrepreneur doit disposer d'un processus pour gérer et surveiller l'accès privilégié à la solution. Il doit notamment:

a) faire respecter et vérifier les autorisations accordées afin d'assurer un accès logique à la solution;
b) accorder et limiter l'accès uniquement aux dispositifs et utilisateurs autorisés ayant un besoin d'accès explicite;
c) surveiller la gestion ou l'accès à distance non autorisé et procéder rapidement à la déconnexion ou à la désactivation en cas d'accès à distance non autorisé;
d) acheminer tous les accès à distance par un nombre limité de points de contrôle d'accès gérés;
e) mettre en œuvre une méthode d'authentification à plusieurs facteurs pour les comptes d'accès privilégié aux centres de données, laquelle doit comporter une séparation appropriée des tâches, l'accès en fonction des rôles et le droit d'accès minimal;
f) autoriser l'exécution des commandes privilégiées et l'accès aux renseignements relatifs à la sécurité uniquement en fonction des besoins opérationnels.

La famille des contrôles d'accès (AC) des PCS fournit de plus amples renseignements sur les exigences en matière de contrôle d'accès. (Voir l'*Appendice G – Sécurité et protection des renseignements personnels*).

5.3.7 Information, données et services de la solution du SGDSL

Dans les 60 jours suivant l'attribution du contrat, l'entrepreneur devra démontrer qu'il respecte l'exigence de SPAC selon laquelle les données, l'information et les services de la ***solution du SGDSL*** doivent être hébergés au Canada dans leur intégralité.

L'entrepreneur doit veiller à ce que le traitement de l'information, les renseignements et les données et les services informatiques demeurent au Canada (voir l'*Appendice G – Sécurité et protection des renseignements personnels*).

5.3.8 Divulgation

Le système d'information ne doit pas transmettre d'information à l'extérieur des limites définies du système ni à un tiers, à moins que des mécanismes et procédures de sécurité de SPAC soient utilisés pour valider le caractère approprié de l'information devant être transmise (voir l'*Appendice G – Sécurité et protection des renseignements personnels).*

5.3.9 Chiffrement

La solution doit protéger toutes les données chiffrées qui sont stockées ou en cours d'acheminement (voir l'*Appendice G – Sécurité et protection des renseignements personnels*). L'entrepreneur doit veiller à ce que toute méthode de chiffrement utilisée pour protéger les données ou en tant que mécanisme d'authentification (p. ex. TLS, modules logiciels, infrastructure à clés publiques [ICP] et jetons d'authentification, au besoin) soit configurée pour une utilisation de concert avec des algorithmes cryptographiques, des longueurs de clés et des cryptopériodes approuvés par le CST.

Les méthodes de chiffrement doivent notamment :

a) utiliser des algorithmes cryptographiques, longueurs de clés et cryptopériodes qui ont été approuvés par le CST et validés par le Programme de validation des algorithmes cryptographiques (CAVP) et qui sont énoncés dans le document ITSP.40.111 ou une version ultérieure;
b) être mises en œuvre dans un module cryptographique validé par le Programme de validation des algorithmes cryptographiques (CAVP) au niveau 1 de validation FIPS (Federal Information Processing Standard) 140-2, et;
c) fonctionner selon le mode de fonctionnement approuvé par la FIPS.

5.3.10 Fuite de données

La solution de l'entrepreneur doit utiliser des contrôles pour veiller à l'isolement approprié des ressources, de sorte que les données de SPAC ne soient pas mêlées à celles d'autres locataires sans qu'il y ait de contrôles compensatoires lorsqu'elles sont utilisées, stockées ou acheminées, et également dans tous les volets de la fonctionnalité et de l'administration du système.

Il doit notamment y avoir des contrôles d'accès et une séparation logique et physique suffisante pour assurer :

a) la séparation des activités administratives internes de l'entrepreneur et des ressources utilisées par SPAC;
b) la séparation des ressources des clients dans les environnements où cohabitent plusieurs locataires, afin d'éviter qu'un client mal intentionné ou compromis puisse nuire au service ou aux données d'un autre client.

5.3.11 Fonctionnalité minimale

L'entrepreneur doit configurer le système d'information afin de permettre uniquement les capacités essentielles (voir l'*Appendice G – Sécurité et protection des renseignements personnels*).

Dans la mesure du possible, l'entrepreneur doit limiter la fonctionnalité des composants à une seule fonction par dispositif et doit désactiver les ports physiques et logiques ou protocoles non utilisés ou inutiles (tels que USB, FTP, IPv6, HTTP).

5.3.12 Réponse en cas d'incident

L'entrepreneur doit travailler avec le coordonnateur de la sécurité de la TI et l'agent de sécurité ministérielle (ASM) de SPAC au confinement et à l'éradication d'une menace pour la sécurité et à la récupération en cas d'incident, conformément aux processus d'intervention en cas d'incident adoptés par l'entrepreneur et par SPAC.

Ainsi, SPAC doit pouvoir suivre l'évolution des cas signalés concernant la sécurité de l'information, demander et obtenir un accès discret à l'information liée aux données de SPAC (données des utilisateurs, relevés des événements du système et des événements liés à la sécurité, saisies de paquets du réseau ou de l'hôte, registres des composantes de sécurité comme les SDI, les SPI, les pare-feux, etc.) sous une forme non chiffrée, aux fins d'enquête. SPAC doit également pouvoir suivre le déroulement des incidents en matière de sécurité de l'information.

L'entrepreneur doit aviser le coordonnateur de la sécurité de la TI de SPAC (par téléphone et par courriel) des événements suspects détectés ou des activités inhabituelles qui pourraient avoir une incidence sur la sécurité.

La famille des réponses en cas d'incident (IR) des PCS fournit de plus amples renseignements sur les rôles et responsabilités de l'entrepreneur en la matière (voir l'*Appendice G – Sécurité et protection des renseignements personnels*).

5.3.13 Vérification

L'entrepreneur doit collaborer avec SPAC pour élaborer et mettre en œuvre les fonctions de vérification, d'analyse et de reddition de comptes. La solution et les services de l'entrepreneur doivent faciliter l'exercice des fonctions de vérification. Entre autres :

a) L'entrepreneur doit donner à SPAC un accès en autonomie à l'information requise aux fins de vérification;
b) L'information relative à la vérification et les outils de vérification doivent être protégée contre tout accès, modification ou suppression non autorisé;
c) Il doit y avoir une capacité de stockage suffisante aux fins de la vérification, afin d'éviter qu'un dépassement de la capacité puisse entraîner la perte ou la réduction de la capacité de vérification;
d) Des avis doivent être envoyés au personnel de l'entrepreneur en cas d'échecs de contrôle, notamment au moyen d'actions automatiques configurées selon les besoins de SPAC et l'envoi d'avis aux intervenants clés lorsque l'utilisation de la capacité atteint 75 %;
e) L'entrepreneur doit aviser SPAC de tout échec de contrôle;
f) La solution doit pouvoir acheminer les incidents et les registres à un système centralisé géré par SPAC (ou un tiers retenu par SPAC) en utilisant des interfaces de production de rapports, des protocoles et des formats de données normalisés, par exemple le CEF (common event format), syslog ou autre format de registre couramment utilisé, ainsi que des API permettant l'extraction à distance de données contenues dans les registres.

La famille de la vérification et de la reddition de comptes (AU) des PCS fournit de plus amples renseignements sur les exigences en matière de vérification (voir l'*Appendice G – Sécurité et protection des renseignements personnels*).

5.3.14 Profil de contrôle de sécurité (PCS)

Le profil de contrôle de sécurité définit les contrôles de sécurité que doit fournir l'entrepreneur et la ***solution du SGDSL***.

L'entrepreneur doit fournir une approche de sécurité globale relativement à la ***solution du SGDSL*** et aux services rendus pendant la durée du contrat.

Pour veiller à la mise en place de contrôles de sécurité adéquats, SPAC a défini un profil de contrôle de sécurité de base à la lumière des contrôles et méthodes énoncés dans le document d'orientation ITSG-33 du Centre de la sécurité des communications (CST) *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (voir l'*Appendice G – Sécurité et protection des renseignements personnels*, *contrôles des PCS).*

5.3.15 Éléments de preuve

Dans le cadre du processus d'évaluation et d'autorisation de sécurité de SPAC, l'entrepreneur doit expliquer en quoi son organisation et/ou la ***solution du SGDSL*** répond au profil de contrôle de sécurité établi. Des éléments probants détaillés sur la conformité de chaque contrôle seront exigés au cours du programme d'évaluation et d'autorisation de sécurité, et le caractère adéquat des éléments probants sera évalué par le coordonnateur de la sécurité de la TI de SPAC.

Voici les exigences relatives à la matrice de traçabilité des exigences relatives à la sécurité (MTERS) de l'entrepreneur ainsi qu'au rapport du spécialiste sous-traitant sur la conformité de la solution en matière d'évaluation et d'autorisation de sécurité (pour de plus amples renseignements, voir l'article 14.2 de l'*Appendice G – Sécurité et protection des renseignements personnels*) :

a) si un contrôle ou un élément ne s'applique pas (S.O.) à la ***solution du SGDSL*** de l'entrepreneur, ce dernier ne doit PAS supprimer l'élément, mais plutôt expliquer en quoi l'élément ne s'applique pas;
b) si le contrôle ou l'élément s'applique à la ***solution du SGDSL*** de l'entrepreneur, mais ne s'applique pas (S.O.) à un partenaire ou sous-traitant, l'entrepreneur doit expliquer en quoi l'élément ne s'applique pas au partenaire ou au sous-traitant;
c) l'entrepreneur doit mentionner si un partenaire ou un sous-traitant est responsable de la mise en œuvre du contrôle;
d) l'entrepreneur doit expliquer en quoi son organisation et la ***solution du SGDSL*** sont conformes au profil de contrôle de sécurité établi.

5.3.16 Attestations de sécurité de la TI

L'entrepreneur doit conserver les attestations et maintenir la conformité aux normes d'audit présentées dans sa soumission pendant toute la durée du contrat.

L'entrepreneur doit, pour toute la durée du contrat, offrir des services d'hébergement fournis soit par lui-même, soit par un prestataire de services sous-traitant titulaire d'une attestation valide, par exemple une attestation ISO 27001/27002:2013, ISO/IEC 27018, FedRAMP. Cette attestation doit avoir été accordée par un organisme de certification reconnu, par exemple un organisme adhérant aux normes du CASCO.

Dans le cas où la conformité à un contrôle de PCS est établie au moyen d'une attestation fournie par un sous-traitant, l'entrepreneur doit fournir une copie du certificat ou du rapport de certification, par exemple une

attestation de vérification d'organisation désignée de niveau « Protégé B » délivrée par Services publics et Approvisionnement Canada (SPAC).

Dans le cas où la conformité à un contrôle de PCS est établie au moyen d'autorisations de sécurité accordées aux employés concernés, l'entrepreneur doit fournir :

a) la liste exhaustive des autorisations accordées aux employés concernés;
b) le nom de l'organisme ayant accordé l'autorisation de sécurité;
c) le numéro de dossier, la date d'entrée en vigueur et la date d'expiration de l'autorisation.

5.3.17 Exigences

Section de l'EDT	Exigence (OBLIGATOIRE)
SEC-MAN- 01	**Emplacement des données et des employés** L'entrepreneur doit démontrer clairement qu'il respecte l'exigence relative à l'emplacement des données, et il doit fournir les plans de déploiement des centres de données, lesquels doivent comprendre des renseignements détaillés concernant : a) les emplacements (pays et ville) des centres de données principaux; b) les emplacements (pays et ville) des centres de données secondaires et des centres de sauvegarde; c) les emplacements (pays et ville) de toutes les composantes d'infrastructure (y compris les serveurs de base de données, les réseaux de stockage et les serveurs d'application); d) les emplacements (pays et ville) des centres de sécurité opérationnels, des centres d'exploitation de réseaux et du bureau de service. L'entrepreneur doit démontrer clairement qu'il respecte l'exigence relative à l'emplacement des entités commerciales et des employés, et il doit indiquer : e) les emplacements (pays et ville) de toutes les entités commerciales exécutant les travaux dans le cadre du contrat; f) les emplacements (pays et ville) de tous les employés exécutant les travaux dans le cadre du contrat.
SEC-MAN-02	**Connexion Web sécurisée** L'entrepreneur doit mettre en œuvre des mesures de protection pour garantir que tous les sites Web et services Web du gouvernement accessibles au public soient configurés de manière à ne fournir le service que par une connexion sécurisée, conformément à l'article 6.2.4 de la Politique sur la gestion de la technologie de l'information et à la Politique sur la sécurité du gouvernement. L'entrepreneur mettra en œuvre une connexion Web sécurisée : • configurée pour HTTPS • pour laquelle HSTS est activé • qui met en œuvre TLS 1.2, ou des versions ultérieures, et utilise des algorithmes et des certificats cryptographiques pris en charge, comme le décrit le CST.

Section de l'EDT	Exigence (OBLIGATOIRE)
	o ITSP.40.062 Conseils sur la configuration sécurisée des protocoles réseau (Section 3.1 Suites de chiffrement AES) o ITSP.40.111 Algorithmes cryptographiques pour les informations non classifiées, protégées A et protégées B • qui désactive les protocoles reconnus comme étant faibles, comme toutes les versions de Secure Sockets Layer (SSL) (p. ex. SSLv2 et SSLv3) et les versions antérieures de TLS (p. ex. TLS 1.0 et TLS 1.1), comme il est recommandé dans l'ITSP.40.062 du CST • désactive les cryptages reconnus comme étant faibles (par ex. RC4 et 3DES)

Section de l'EDT	Exigence (COTÉE)
SEC-03	**Politiques et procédures de sécurité de la TI (contrôles)** L'entrepreneur doit démontrer qu'il est en mesure de se conformer aux exigences relatives à la sécurité de la TI par le respect de politiques et procédures qui contribuent à la sécurité de la TI pendant toute la durée du contrat en fournissant des éléments probants pour étayer toute politique ou procédure existante qui favorise les familles de contrôle de sécurité décrites à l'appendice G et dans le document ITSG-33. L'entrepreneur devrait décrire en quoi ses politiques et procédures cadrent avec les familles de contrôle de sécurité, en fournissant l'information suivante concernant ses politiques et procédures en vigueur : (a) le nom de la politique ou de la procédure; (b) son objectif; (c) sa portée; (d) les rôles et responsabilités y étant décrits; (e) la façon dont elle assure la coordination entre les entités organisationnelles; (f) La façon dont elle assure la conformité au sein de l'organisation. Remarque : L'entrepreneur devrait fournir suffisamment de détails sur ses politiques et procédures pour permettre au Canada de faire une évaluation de la réponse dans son intégralité.
SEC-04	**Diagramme de la topologie de la sécurité de la TI** Le soumissionnaire devrait fournir un diagramme de la topologie de la sécurité de la TI, qui devrait porter sur les éléments suivants : a) les interfaces – puce distincte pour chaque catégorie; b) le Web; c) les applications; d) les bases de données; e) les dispositifs de sécurité; f) la gestion du système; g) l'infrastructure de sauvegarde.

Section de l'EDT	Exigence (COTÉE)
SEC-05	**Organisation de sécurité** L'entrepreneur devrait décrire l'expérience de l'organisation de sécurité qui assurera la sécurité du SGDSL. La description doit préciser le nom de chaque personne, son rôle, ses fonctions, son expérience et ses attestations.
SEC-06	**Séparation des données** L'entrepreneur devrait présenter la stratégie qu'il propose à l'égard de la séparation des données, notamment en ce qui concerne : a) les documents sur la conception du système d'information; b) l'architecture du système d'information; c) les processus et procédures de séparation des données.
SEC-07	**Élimination et nettoyage des données** L'entrepreneur devrait présenter la stratégie qu'il propose à l'égard de l'élimination et du nettoyage des données du Canada, y compris : a) un plan de nettoyage de disques durs ou un plan d'action si le système est hébergé dans un environnement virtuel qui garantira que les données du Canada ne sont pas accessibles; b) un plan d'élimination des données; c) les processus et procédures d'élimination du système; d) un plan de destruction des documents en double qui peuvent être stockés dans un système de gestion des documents ou de secours, et; e) le processus qu'il prévoit suivre lorsque le système ne sera plus requis et sera mis hors service.
SEC-08	**Service de surveillance continue** L'entrepreneur devrait présenter l'approche qu'il propose à l'égard de la surveillance continue [du SGDSL] et inclure les éléments suivants : a) la stratégie de surveillance continue; b) les mesures, les paramètres et les fréquences d'évaluation de la surveillance et du contrôle de l'état établis; c) des détails sur la collecte de données et ses volets relatifs à l'établissement de rapports; d) les méthodes d'analyse des données recueillies et des conclusions des rapports assorties de recommandations; e) les mécanismes de réponse aux résultats de l'évaluation qui doivent comprendre la prise de décisions quant à l'atténuation des vulnérabilités techniques, opérationnelles et de gestion, à l'acceptation du risque ou au transfert du risque à un autre responsable, et; f) les cycles d'examen et de mise à jour pour favoriser l'amélioration continue et l'évolution des capacités de mesure.
SEC-09	**Attestation de sécurité de la TI de l'industrie** L'entrepreneur devrait fournir une copie valide de ses attestations de sécurité et normes d'audit applicables à la solution proposée comme preuve de ses attestations de sécurité et normes d'audit, et décrire la façon dont chaque attestation de sécurité de la TI et norme d'audit, telles que les suivantes, a été évaluée et obtenue :

Section de l'EDT	Exigence (COTÉE)
	a) FedRAMP; b) Cloud Security Alliance – programme STAR; c) COBIT; d) ISO 27001; e) PCI DSS; f) CMM; g) autres. L'entrepreneur devrait également préciser si l'attestation ou la norme d'audit s'applique à l'ensemble ou à une partie de la solution.
SEC-10	**Gestion de l'identité, des justificatifs d'identité et de l'accès** L'entrepreneur devrait fournir des détails sur les capacités relatives au niveau d'assurance de la solution de gestion de l'identité, des justificatifs d'identité et de l'accès qu'il propose en ce qui concerne la Norme sur l'assurance de l'identité et des justificatifs du Secrétariat du Conseil du Trésor. L'entrepreneur devrait indiquer le niveau d'assurance et démontrer en quoi il satisfait aux exigences de ce niveau.

5.4 GESTION DES SERVICES

5.4.1 Contexte

La gestion des services est l'approche stratégique relative à la conception, à la réalisation, à la gestion et à l'amélioration de la façon dont la TI sera utilisée dans la ***solution du SGDSL***. L'objectif de la gestion des services consiste à garantir que les processus, les employés et la technologie adéquats sont en place pour permettre à la ***solution du SGDSL*** d'atteindre les objectifs opérationnels de SPAC. La gestion des services est associée à l'ITIL, un cadre de travail qui fournit des pratiques exemplaires pour harmoniser la TI avec les besoins opérationnels.

L'entrepreneur doit gérer ses services de TI et déployer un ensemble de ressources spécialisées et de capacités équivalentes à celles prescrites dans le cadre de l'ITIL comme source de pratiques exemplaires en matière de gestion des services. Le cadre doit mettre l'accent sur l'importance de la coordination et du contrôle dans les divers processus, systèmes et fonctions nécessaires à la gestion du cycle de vie complet des services de TI, y compris l'élaboration, la conception, la transition, l'exploitation et l'amélioration continue des stratégies – c'est-à-dire le cycle de vie de la gestion des services de TI.

L'entrepreneur doit fournir au chargé de projet des rapports de vérification réalisés selon les exigences de SPAC par un organisme indépendant et faisant état de l'harmonisation avec les pratiques exemplaires, des mesures prises pour corriger les lacunes et du maintien de la conformité.

L'entrepreneur doit adapter le guide de l'ITIL (ou un cadre similaire) à l'appui de l'environnement du SGDSL, et il doit continuellement déployer ces pratiques pendant toute la durée du contrat.

5.4.2 Service de gestion des services de TI : gestion des incidents, des problèmes, des changements et des versions

Le tableau suivant énonce les pratiques exemplaires, les processus généraux et les activités que l'entrepreneur devrait offrir en collaboration avec SPAC afin de gérer les incidents, les problèmes, les changements et les versions liés au service de gestion des services de TI :

Processus	Activités (étapes)
1.0 Gestion des incidents	a) Détection de l'incident b) Consignation de l'incident c) Catégorisation de l'incident d) Hiérarchisation de l'incident e) Analyse et diagnostic f) Acheminement à un autre niveau de soutien g) Suivi h) Communication avec le personnel de soutien technique de SPAC tout au long de l'incident i) Résolution de l'incident j) Clôture de l'incident et rapports
2.0 Gestion des problèmes	a) Détection du problème b) Consignation du problème c) Catégorisation du problème d) Hiérarchisation du problème e) Enquête sur le problème, analyse et diagnostic f) Création d'un dossier d'erreur connue g) Communication avec le personnel de soutien technique de SPAC tout au long de l'incident h) Résolution du problème i) Clôture et rapports et examen des problèmes majeurs
3.0 Gestion des changements	a) Création d'une demande de changement b) Examen et évaluation de la demande de changement c) Soutien à la gestion du changement d) Évaluation du changement par le gestionnaire du changement e) Évaluation du changement par le Comité consultatif sur les changements f) Planification du changement et autorisation de conception g) Évaluation et mise en œuvre du changement h) Mise à l'essai du changement i) Autorisation de mise en œuvre du changement j) Mise en œuvre du changement k) Examen après la mise en œuvre et fermeture du dossier de changement

Processus	Activités (étapes)
4.0 Gestion des versions	a) Soutien à la gestion des versions b) Planification de la version et de sa mise en œuvre c) Production et essai de la version d) Déploiement de la nouvelle version e) Soutien initial f) Examen et clôture du dossier de mise en œuvre de la version

5.4.3 Exigences relatives aux niveaux de service

5.4.3.1 Mesure du rendement et établissement de rapports

L'entrepreneur doit soumettre au chargé de projet un rapport sur le rendement de la ***solution du SGDSL*** par rapport aux exigences définies dans l'énoncé des travaux.

Ce rapport doit contenir l'identificateur et l'état de la demande de service, ainsi que tout renseignement dont le chargé de projet aura besoin pour comprendre la demande et la régler.

5.4.3.2 Lacunes et exclusions relatives aux normes de service

En ce qui concerne les lacunes relatives aux normes de service ou une tendance négative donnant à penser qu'il y aura non-respect des normes de service, à la suite d'une analyse des données saisies dans le rapport sur le rendement, l'entrepreneur doit indiquer toutes les lacunes et faire ce qui suit :

a) aviser le chargé de projet dès qu'il prend connaissance de ces lacunes;
b) effectuer une analyse des causes fondamentales afin de trouver la cause sous-jacente des lacunes et de préserver les données qui indiquent la cause des lacunes;
c) prendre des mesures visant à réduire au minimum les répercussions des lacunes et à empêcher que celles-ci se reproduisent, comme il a été convenu avec le chargé de projet;
d) si cela est possible, corriger les lacunes immédiatement afin de reprendre la prestation du service conformément à la norme de service applicable;
e) préparer un rapport qui fait état des lacunes et, dans la mesure du possible, de la cause, des répercussions sur les activités, des plans de mesures correctives, du calendrier de mise en œuvre des plans d'amélioration et de toute incidence sur les services, et le remettre au chargé de projet;
f) aviser le chargé de projet de l'état d'avancement de toutes les mesures correctives qu'il a prises en ce qui concerne la cause sous-jacente des lacunes;
g) dans la détermination de sa conformité avec les normes de service, ne pas tenir compte des problèmes de rendement :
    i. entraînés par des facteurs indépendants de sa volonté, découlant de mesures que le gouvernement du Canada (GC) ou des tiers ont prises ou n'ont pas prises indépendamment de sa volonté;
    ii. découlant du matériel de SPAC et/ou d'un tiers sur lequel il n'exerce pas de contrôle principal (sauf si l'événement est le résultat d'actes ou d'omissions de sa part).

À la demande de SPAC, l'entrepreneur doit fournir une justification que la cause du problème lié au service est raisonnablement hors de son contrôle.

5.4.4 Normes de service

5.4.4.1 Disponibilité des applications

Ce niveau de service mesure la disponibilité de la ***solution du SGDSL***.

DISPONIBILITE DES APPLICATIONS		
Mesure du service	**Objectif de rendement**	**Pourcentage de rendement par rapport aux ANS**
a) Pourcentage	Pourcentage du temps où l'application est disponible dans le cadre des activités opérationnelles habituelles. (24 heures sur 24, 7 jours par semaine)	Applications de production : 97,0 %
b) Formule	[Nombre de minutes durant un mois où les applications de production et leurs différentes composantes fonctionnaient sans qu'aucun incident de priorité 1 ou 2 relevant du contrôle de l'entrepreneur n'ait été signalé] divisé par [Nombre total de minutes durant ce mois moins (nombre de minutes de la période de maintenance + temps d'arrêt prévu)] × 100 = [Pourcentage du temps où l'application était disponible durant le mois visé].	
c) Intervalle de mesure	Mois civil	
d) Période de référence	Mois civil	
e) Méthode de mesure et données de base	L'outil fourni par l'entrepreneur enregistre automatiquement l'horodatage de chacune des activités dans le cadre d'un processus, y compris soit les données relatives au temps de disponibilité, soit celles relatives au temps d'arrêt.	

5.4.4.2 Rapports de l'entrepreneur

Ce niveau de service établit la mesure dans laquelle l'entrepreneur respecte le calendrier de production de rapports convenu et les exigences relatives à l'exactitude des rapports, tel qu'il est énoncé dans l'EDT.

RAPPORTS		
Mesure du service	**Objectif de rendement**	**Pourcentage de rendement par rapport aux ANS**
a) Calendrier de production des rapports	Rapports remis dans les délais prévus au titre du contrat, tel qu'il est énoncé dans l'EDT	95 %
b) Formule	Le respect du calendrier (en pourcentage) correspond au nombre de mesures convenues réalisées dans les délais prévus, divisé par le nombre total de mesures convenues durant la période visée. L'exactitude des données (en pourcentage) correspond au nombre de données individuelles des rapports qui correspondent aux données réelles, divisé par le nombre total de données contenues dans les rapports présentés durant le mois.	

RAPPORTS	
c) Intervalle de mesure	Mois civil
d) Période de référence	Mois civil
e) Méthode de mesure et données de base	À déterminer par SPAC en consultation avec l'entrepreneur après l'attribution du contrat.

5.4.4.3 Disponibilité du bureau de service du SGDSL de l'entrepreneur

DISPONIBILITÉ DU BUREAU DE SERVICE		
Mesure du service	**Objectif de rendement**	**Pourcentage de rendement par rapport aux ANS**
a) Horaire	À déterminer par le GC en consultation avec l'entrepreneur après l'attribution du contrat	95 %
b) Formule	Disponibilité (%) = 100 % - Non-disponibilité où la non-disponibilité est définie comme suit : (Σ Durée de l'interruption × 100 %) ÷ (Horaire - Interruption prévue)	
c) Intervalle de mesure	Premier mois : mesure quotidienne Par la suite : mesure quotidienne	
d) Période de référence	Premier mois : rapport hebdomadaire Par la suite : rapport mensuel	
e) Méthode de mesure et données de base	À déterminer par SPAC en consultation avec l'entrepreneur après l'attribution du contrat.	

5.4.4.4 Délai d'acceptation des incidents par le bureau de service du SGDSL de l'entrepreneur

Le délai d'acceptation des incidents est une mesure du temps nécessaire pour que le bureau de service accepte (c.-à-d. reçoive, consigne et attribue aux fins de résolution) un incident. Le délai est calculé à partir du moment où l'incident est reçu par l'entrepreneur jusqu'au moment où l'incident est consigné et attribué aux fins de résolution dans l'application du bureau de service.

DÉLAI D'ACCEPTATION DES INCIDENTS		
Mesure du service	**Objectif de rendement**	**Pourcentage de rendement par rapport aux ANS**
a) Pourcentage	Incident de priorité 1 : 60 minutes ou moins Incident de priorité 2 : 60 minutes ou moins Incident de priorité 3 : 2 heures normales d'exploitation ou moins	90 % ou plus (tous les niveaux de priorité)

DÉLAI D'ACCEPTATION DES INCIDENTS		
	Incident de priorité 4 : 4 heures normales d'exploitation ou moins	
b) Formule	[Nombre d'incidents (tous les niveaux de priorité) reçus et acceptés (c.-à-d. reçus, consignés et attribués) dans le respect de l'objectif de rendement pendant l'intervalle de mesure] divisé par Nombre total d'incidents (tous les niveaux de priorité) reçus et acceptés pendant l'intervalle de mesure × 100 % = Pourcentage atteint	
c) Intervalle de mesure	Mois civil	
d) Période de référence	Mois civil	
e) Méthode de mesure et données de base	À déterminer par le GC en consultation avec l'entrepreneur après l'attribution du contrat.	

5.4.4.5 Exigences relatives à l'entrepreneur

SECTION DE L'EDT	Exigence (OBLIGATOIRE)
SRV-STD-01	La maintenance prévue doit avoir lieu entre 24 h vendredi et 6 h lundi, heure normale de l'Est.
SRV-STD-02	Dans le cas d'une maintenance non planifiée, l'entrepreneur doit obtenir l'approbation du responsable technique quant au moment où cette maintenance non planifiée pourra avoir lieu.
SRV-STD-03	S'il doit effectuer une maintenance d'urgence, l'entrepreneur en avisera immédiatement, par écrit, le responsable technique, qui doit approuver les travaux de maintenance avant leur exécution.

5.4.5 Bureau de service

5.4.5.1 Contexte

Le bureau de service est le point d'entrée et de contact unique pour les clients et les utilisateurs. Il s'agit d'une fonction essentielle pour résoudre les problèmes, rétablir le service normal le plus rapidement possible et réduire au minimum les effets négatifs sur les activités et garantir le maintien du meilleur niveau de service possible sur le plan de la qualité et de la disponibilité.

La gestion des incidents traite tous les incidents, lesquels surviennent sous différentes formes et peuvent découler de problèmes d'applications, de matériel et de réseau et qui doivent tous être résolus rapidement pour minimiser l'incidence sur les activités.

Les incidents sont généralement traités dès qu'ils sont signalés (réactif). Toutefois, selon la nature, la complexité et l'incidence du problème, il pourrait être nécessaire de porter le problème à l'attention d'autres niveaux de soutien (ou paliers) pour résolution.

Grâce au processus de gestion des incidents, une approche plus proactive peut être adoptée pour résoudre les incidents récurrents dont la cause profonde est inconnue à l'aide du processus de gestion de problèmes.

Les activités clés du processus de gestion des problèmes visent à établir la cause profonde des incidents relevés par le processus de gestion des incidents, et à trouver la façon de résoudre ou de contourner ces problèmes.

Une fois cette étape terminée, la solution ou la solution de rechange est mise en œuvre grâce aux procédures de contrôle appropriées de gestion des changements et des versions.

5.4.5.2 Objectifs

Les processus de gestion des incidents, des problèmes et des changements visent à :

a) rétablir les opérations normales du service aussi rapidement que possible et minimiser les répercussions nuisibles sur les opérations;
b) prévenir les problèmes et les incidents qui en découlent;
c) éliminer les incidents récurrents;
d) limiter au maximum les répercussions des incidents ne pouvant pas être prévenus;
e) minimiser l'incidence négative des changements mis en œuvre;
f) offrir aux clients une expérience de qualité supérieure de façon répétée, ainsi qu'adopter un processus normalisé et utiliser des outils élaborés en fonction des pratiques exemplaires de l'industrie;
g) définir et mesurer les indicateurs de rendement clés qui stimuleront les améliorations des processus.

5.4.5.3 Gestionnaire de services

L'entrepreneur doit mettre un gestionnaire de services à la disposition des représentants de SPAC pendant les jours ouvrables, de 8 h à 17 h (heure de l'Est), pour régler les questions relatives aux activités de mise en œuvre des versions, à la planification de la maintenance des versions et au calendrier des versions, à la qualité du service, à la transmission des services de gestion à un autre palier hiérarchique (incidents) et à la production de rapports. Le gestionnaire doit pouvoir être joint en dehors des heures de bureau pour les incidents portant un niveau de priorité élevé, les urgences et les incidents de sécurité.

5.4.5.4 Structure du bureau de service

L'entrepreneur doit fournir et maintenir un bureau de service bilingue (français et anglais) accessible (voir le tableau ci-après) au personnel de soutien technique de SPAC en vue d'examiner et de résoudre les problèmes liés à la ***solution du SGDSL*** ou à un tiers, ainsi que de les porter à l'attention des responsables pertinents.

Niveau de soutien	Semaine	Heures normales de travail (HNE)	Après les heures (HNE)	Fin de semaine	Après les heures (HNE)
Niveau de soutien 1 de SPAC	Du lundi au vendredi	De 8 h à 17 h	De 17 h à 8 h	Du vendredi au lundi	De 17 h à 8 h
Niveau de soutien 2 de SPAC					

Niveau de soutien 3 de l'entrepreneur*					
* Entrepreneur – Soutien relatif à la ***solution du SGDSL*** et à tous outils d'un sous-traitant, d'un partenaire ou d'un tiers.					

5.4.5.5 Exigences relatives au bureau de service

SECTION DE L'EDT	**Exigence (OBLIGATOIRE)**
SRV-DESK-01	L'entrepreneur doit avoir un bureau de service joignable sans frais par téléphone, par courriel et par un moyen de communication sur site Web afin de répondre aux incidents et aux demandes de services (« demandes de soutien »). Le responsable technique fournira à l'entrepreneur une liste d'au plus XX utilisateurs qui sont autorisés à soumettre des demandes de soutien.
SRV-DESK-02	L'entrepreneur doit fournir et maintenir un bureau de service bilingue (anglais du Canada et français du Canada) accessible à SPAC pour fournir du soutien et faciliter l'utilisation de la ***solution du SGDSL***, pour répondre aux demandes de renseignements, aux demandes de soutien pour des questions liées aux réseaux, au matériel, aux logiciels, aux bases de données et à la gestion de la sécurité, pour résoudre les perturbations de service et aider les utilisateurs aux prises avec un mauvais fonctionnement de certaines caractéristiques ou fonctions.
SRV-DESK-03	Le bureau de service doit collaborer avec le personnel de soutien technique de SPAC afin de résoudre les problèmes liés au SGDSL, y compris les outils de l'entrepreneur et les outils tiers de SPAC et les systèmes de SPAC intégrés dans la ***solution du SGDSL***.
SRV-DESK-04	L'entrepreneur doit collaborer avec SPAC pour déterminer la structure, les processus et les procédures de soutien qui seront utilisés pour gérer l'acheminement aux paliers hiérarchiques supérieurs, les incidents, les problèmes et les changements, conformément à un modèle convenu.
SRV-DESK-05	L'entrepreneur doit définir et appliquer des processus de soutien en ce qui concerne la gestion de l'acheminement aux paliers hiérarchiques supérieurs, des incidents, des problèmes et des changements.
SRV-DESK-06	L'entrepreneur doit mettre au point un système de dossiers d'incident pour assurer le suivi des demandes de soutien.

SECTION DE L'EDT	**Exigence (COTÉE)**
SRV-DESK-07	Le système de dossiers d'incident devrait pouvoir offrir au moins les fonctions suivantes : a) un numéro de suivi unique; b) un avis automatique communiqué par courriel à l'utilisateur autorisé ayant généré la demande de soutien lorsque le dossier d'incident a été mis à jour, modifié ou transmis à un palier hiérarchique supérieur; c) la capacité de produire un rapport mensuel de tous les dossiers d'incident créés durant le mois, y compris les renseignements énumérés à l'article 5.5.4.3; d) la capacité de produire des rapports supplémentaires à la demande de SPAC dans les cinq jours civils suivant une telle demande;

SECTION DE L'EDT	Exigence (COTÉE)
	e) l'envoi de messages à diffusion générale ou d'autres avis pour faire le point sur les événements prévus et imprévus.
SRV-DESK-08	Le système de dossiers d'incident devrait contenir au moins les renseignements suivants : a) la date et l'heure auxquelles la demande a été formulée; b) le nom de la personne qui a soumis la demande de soutien; c) le nom de la personne qui a consigné la demande; d) le niveau de gravité de la demande de soutien selon l'entrepreneur; e) les procédures à suivre convenues avec le responsable technique; f) une description de l'incident; g) des détails sur les services touchés; h) la durée de l'interruption, le cas échéant; i) le temps requis pour résoudre le problème; j) des commentaires; k) la date et l'heure auxquelles le problème a été résolu.
SRV-DESK-09	Le système de dossiers d'incident devrait pouvoir générer des rapports : a) la production d'un rapport sur le rendement du bureau de service afin de démontrer le degré de respect des exigences relatives aux niveaux de service et de l'accord sur les niveaux de service; b) la capacité de produire un rapport mensuel de tous les dossiers d'incident créés durant le mois, y compris les renseignements énumérés à l'article 5.5.4.3; c) la capacité de produire des rapports supplémentaires à la demande de SPAC dans un délai déterminé, par exemple cinq (5) jours civils suivant une telle demande; d) la gestion et le suivi de l'utilisation du bureau de service et la production de rapports connexes; e) un ensemble de rapports normalisés, comme des rapports sur la gestion des incidents, des rapports sur la gestion des problèmes et des rapports sur les services qui ont déjà été configurés en vue d'une utilisation facile et rapide.
SRV-DESK-10	Le bureau de service de l'entrepreneur devrait disposer de ressources ayant les autorisations de sécurité suffisantes et possédant une bonne connaissance des ***langues officielles du Canada***.
SRV-DESK-11	Au cours des incidents prévus ou imprévus, l'entrepreneur devrait fournir toutes les ressources et le personnel qualifiés nécessaires disposant des autorisations de sécurité suffisantes et des connaissances linguistiques appropriées.
SRV-DESK-12	L'entrepreneur devrait fournir toutes les ressources et le personnel qualifiés nécessaires disposant des autorisations de sécurité suffisantes et des connaissances linguistiques appropriées pour soutenir et exploiter le bureau de service bilingue.
SRV-DESK-13	Le bureau de service de l'entrepreneur devrait disposer du personnel technique dûment formé afin d'assurer le soutien des niveaux 1, 2 et 3 et l'acheminement au palier hiérarchique approprié, y compris à des tiers, en vue de la résolution des demandes, des incidents et des problèmes.
SRV-DESK-14	L'entrepreneur devrait avoir des procédures consignées concernant les opérations et l'administration du bureau de service.
SRV-DESK-15	L'entrepreneur devrait tenir une liste à jour des personnes-ressources responsables de l'acheminement aux paliers hiérarchiques supérieurs pour tous les niveaux de service (y compris les tiers) pendant toute la durée du contrat, et fournir cette liste sur demande à SPAC.

SECTION DE L'EDT	Exigence (COTÉE)
SRV-DESK-16	L'entrepreneur devrait fournir un processus de gestion des incidents en boucle fermée et pouvoir communiquer avec le personnel de soutien technique et les utilisateurs de SPAC, afin de les informer des changements d'état ou de leur demander de plus amples renseignements, au besoin.
SRV-DESK-17	L'entrepreneur devrait fournir le nombre des problèmes signalés par le personnel de soutien de SPAC après les heures (voir la section 5.4.5.4 – Structure du bureau de service).

5.4.5.6 Premier point de contact

L'entrepreneur doit être le premier point de contact pour l'ensemble des incidents, des problèmes et des communications générales portés à son attention par le personnel de soutien technique de SPAC, et fournir les services de soutien comprenant ce qui suit :

a) effectuer l'identification, l'enregistrement, la catégorisation, la priorisation, le diagnostic initial, l'acheminement à d'autres niveaux de soutien, la résolution, la clôture et la communication avec le personnel de soutien technique à chacune des étapes de l'incident;
b) restaurer le plus rapidement possible le fonctionnement normal des services en cas d'interruption de ceux-ci;
c) appuyer le personnel de soutien technique du GC en gérant la communication et en acheminant les incidents et les demandes au palier hiérarchique supérieur à l'aide des procédures définies;
d) résoudre les incidents liés aux problèmes associés aux logiciels, au matériel et aux réseaux;
e) réagir aux incidents relatifs à l'application et fournir un soutien quant à la façon de faire;
f) fournir un soutien relatif aux justificatifs de connexion fournis par l'entrepreneur (le cas échéant), y compris des capacités libre-service de réinitialisation du mot de passe, des demandes de changement des privilèges d'accès ainsi que des demandes d'activation, de suspension et de fermeture de comptes d'utilisateurs;
g) résoudre les problèmes liés à la cause inconnue d'un ou de plusieurs incidents;
h) accorder un accès au premier point de contact au moyen d'un numéro de téléphone sans frais, d'une adresse électronique, du libre-service, du clavardage en direct et d'un système de gestion des demandes pour tous les services du bureau de service décrits dans le présent Énoncé des travaux;
i) Fournir divers modes de prestation de services de soutien aux utilisateurs (voir la section 5.5.5.6 – Modes de prestation de services de soutien aux utilisateurs (MPSSU);
j) Modes de prestation de services de soutien aux utilisateurs (MPSSU).

L'entrepreneur doit fournir un bureau de service accessible et disponible dans tous les fuseaux horaires du Canada et offrant différents modes de prestation de soutien, comme ceux qui suivent :

SECTION DE L'EDT	Exigence (COTÉE)
SRDC-TEL-01	**Téléphone** L'entrepreneur devrait fournir un numéro de téléphone local et un numéro de téléphone sans frais pour permettre au personnel de soutien technique de SPAC de s'adresser directement au personnel de soutien du bureau de service pour soumettre et régler leurs demandes de soutien, notamment pour ce qui concerne les demandes de renseignements, les marches à suivre et les incidents qui touchent le service.

SECTION DE L'EDT	Exigence (COTÉE)
SRDC-AA-02	**Système d'aide vocale** L'entrepreneur devrait fournir un système d'aide vocale offrant un éventail d'options en libre-service au personnel de soutien technique, aux clients et aux utilisateurs de SPAC.
SRDC-AA-02.1	Le système d'aide vocale devrait être fourni dans les ***langues officielles du Canada***, 24 heures sur 24, sept jours par semaine.
SRDC-AA-02.2	Le personnel de soutien technique de SPAC devrait avoir la possibilité de parler au personnel de soutien du bureau de service à tout moment pendant les heures de fonctionnement du bureau.
SRDC-AA-02.3	Le système d'aide vocale devrait comprendre ce qui suit a) réponse rapide : répondre à tous les appels à la première sonnerie; b) service aux utilisateurs : offrir un service tous les jours, 24 heures sur 24; c) réacheminement des appels : offrir un menu simple pour réacheminer les appelants vers le numéro de téléphone approprié ou l'information enregistrée pertinente sans aide personnelle. L'information enregistrée peut être mise à jour en tout temps à partir de n'importe quel téléphone, et elle est protégée par un mot de passe; d) service de messagerie : maintenir un appel à un poste en particulier si la ligne est occupée, annoncer la position de l'appelant dans la file d'attente et offrir les options de demeurer dans la file d'attente, de laisser un message, de laisser un numéro à rappeler ou de raccrocher et d'essayer de rappeler plus tard; e) capacité d'exécuter des fonctions administratives, de fournir une aide pratique aux utilisateurs grâce à un accès aux bases de connaissances et de vérifier l'état des incidents en ligne.
SRDC-EML-03	**Courriel** Fournir une adresse électronique ou un formulaire Web pour permettre au personnel de soutien technique ou aux utilisateurs de SPAC de se servir de leur système de messagerie électronique pour signaler des incidents.
SRDC-EML-03.1	L'entrepreneur devrait fournir une confirmation et des avis par courriel au personnel de soutien technique et aux utilisateurs de SPAC qui communiquent avec le bureau de service par courriel.
SRDC-LIVE-04	**Clavardage en direct** L'entrepreneur devrait proposer un service de clavardage pour permettre au personnel de soutien technique de SPAC d'amorcer un dialogue texte.
SRDC-DISA-05	**Personnes handicapées** L'entrepreneur devrait fournir aux clients d'autres formats de communication et de services axés sur la clientèle, selon les besoins.
SRDC-DISA-05.1	L'entrepreneur devrait veiller à ce que la technologie du bureau de service soit mise à niveau, puis intégrée au service à la clientèle général du BT.
SRDC-FAQ-06	**Foire aux questions** La ***solution du SGDSL*** devrait permettre au personnel de soutien technique de SPAC de se reporter à une foire aux questions pouvant tirer profit d'une base de connaissances.

5.4.5.7 Niveau de priorité, incidence opérationnelle et description de l'incident

Le tableau suivant décrit les niveaux de priorité, l'incidence opérationnelle et la description des incidents

Niveau de priorité		Incidence opérationnelle	Description
P1	Critique	Incidence critique sur les activités ou l'intérêt national	L'incident a entraîné un arrêt total et immédiat du travail, ce qui a eu une incidence sur une fonction essentielle ou une composante essentielle de l'infrastructure, ainsi que sur un processus opérationnel principal ou un vaste groupe d'utilisateurs. Il n'existe aucune solution de rechange. Exemples : a) problèmes majeurs liés à une application (p. ex. catalogage, sélection des fournisseurs, etc.); b) interruption grave pendant des périodes critiques (p. ex. traitement de fin de l'exercice financier); c) panne réseau; d) infraction ou manquement à la sécurité. Par ailleurs, le niveau de priorité 1 doit être attribué à des incidents liés à l'intérêt national.
P2	Élevée	Incidence opérationnelle majeure	Un processus opérationnel est touché d'une manière qui fait que des fonctions opérationnelles sont gravement affaiblies, plusieurs utilisateurs sont touchés, un utilisateur autorisé important est touché, ou la capacité ou la fonctionnalité d'une composante essentielle est considérablement réduite. Une solution de rechange peut exister, mais elle n'est pas facilement viable. Exemples : a) problèmes majeurs liés à des données, à une base de données ou à une application; b) fonctionnement au ralenti du système, mais charge de travail gérable. Atteinte à la sécurité d'un système non essentiel.
P3	Moyenne	Incidence opérationnelle modérée	Un processus opérationnel est touché d'une manière qui fait que certaines fonctions ne peuvent pas être utilisées par les utilisateurs ou que *la solution SGDSL* ou un service est affaibli. Une solution de rechange peut exister.

Niveau de priorité		Incidence opérationnelle	Description
P4	Faible	Incidence opérationnelle minimale	L'incident a peu d'incidence sur les processus opérationnels normaux et peut être résolu selon un calendrier établi. Une solution de rechange existe ou l'incident a une incidence négative minimale sur la capacité d'un utilisateur à effectuer ses tâches quotidiennes normales. Exemples : a) questions pratiques sur les procédures; b) demandes de service (p. ex. amélioration d'un système; *c)* problèmes liés aux périphériques (p. ex. imprimante locale d) maintenance préventive.

5.4.5.8 Intervention en cas d'incident, cibles de résolution et niveaux de service

Le tableau suivant indique les niveaux de priorité des incidents ainsi que la réponse, le délai de réponse et d'accusation de réception ciblé, le délai de résolution ciblé et la cible de service pour chacun.

Niveau de priorité		Réponse	Délai de réponse et d'accusation de réception ciblé	Délai de résolution ciblé	Cible de service**
P1	Critique	Effort immédiat et maintenu, faisant appel à toutes les ressources disponibles **jusqu'à** la résolution. Procédures de recours aux employés sur appel activées, soutien du fournisseur.	30 minutes; 24x7	6 heures	90 %
P2	Élevée	L'équipe de soutien répond immédiatement, évalue la situation, pourrait interrompre le travail des autres membres du personnel qui travaillent à des tâches de priorité normale ou modérée afin d'obtenir leur *aide*.	1 heure; 24x7	1 jour ouvrable	90 %
P3	Moyenne	Répondre en appliquant les procédures courantes et en agissant conformément aux structures de gestion normales de supervision	4 heures ouvrables; 12x5	2 jours ouvrables	90 %
P4	Faible	Répondre en appliquant les procédures opérationnelles, si le temps le permet	6 heures ouvrables; 12x5	5 jours ouvrables	90 %
** Les niveaux de service sont mesurés en fonction des heures normales de bureau (entre 8 h et 17 h), sauf pour le niveau P1 qui est mesuré en fonction d'une journée de 24 heures.					

5.4.5.9 Gestion des problèmes et des incidents

L'entrepreneur doit gérer problèmes et les incidents liés à la ***solution du SGDSL*** afin de s'assurer que les services sont rétablis rapidement, notamment en effectuant les tâches suivantes :

a) recommander des procédures relatives à la gestion des incidents qui s'inspirent des processus de l'ITIL ou des processus ISO;
b) veiller à ce que les réponses au personnel de soutien technique de SPAC soient fondées sur l'ordre de priorité et l'incidence plutôt que sur la méthode utilisée pour aviser le bureau de service (p. ex., téléphone, courriel, télécopieur);
c) Acheminer au bureau de service de l'entrepreneur les problèmes et les incidents au moyen d'un processus défini et convenu;
d) fournir un système permettant de consigner, de gérer et de suivre l'ensemble des incidents, des rapports d'incident, des demandes de renseignements, peu importe les moyens par lesquels les incidents sont soumis.
e) fournir un processus de bout en bout qui permet de repérer les incidents, de les acheminer au palier hiérarchique approprié, de les transférer, de les résoudre (gérer) et de les clore, y compris ceux qui sont acheminés à des tiers;
f) recevoir les demandes que les utilisateurs et le personnel de soutien technique de SPAC présentent par téléphone, par courriel, au moyen du libre-service, par clavardage en direct et par le système de gestion des demandes, y répondre, résoudre les problèmes, assurer un suivi, et effectuer une surveillance jusqu'à la clôture;
g) veiller à ce que tous les incidents soient désignés par un numéro unique, peu importe la méthode de communication utilisée, pour qu'il soit possible d'assurer leur suivi pendant le cycle de vie de la demande de service;
h) appliquer les pratiques exemplaires du processus de gestion des problèmes afin de :
    i. veiller à ce que les incidents récurrents qui répondent aux critères définis soient examinés dans le cadre du processus d'analyse des causes fondamentales;
    ii. consigner les solutions aux incidents récurrents dans la base de connaissances, à l'exception des incidents de sécurité;
i) vérifier l'acceptation des services en communiquant avec le personnel de SPAC pour confirmer les résultats et le niveau de satisfaction;
j) fournir l'autorisation du personnel de soutien de SPAC pour la clôture des demandes de service et des incidents signalés au bureau de service;
k) accorder à SPAC un accès complet et continu à tous les renseignements sur la clôture des problèmes, des incidents et des demandes, notamment des renseignements sur :
    i. la réception des problèmes et des incidents,
    ii. la désignation des problèmes et des incidents,
    iii. l'enregistrement, le suivi et la mise à jour des problèmes et des incidents,
    iv. la catégorisation des problèmes et des incidents,
    v. la priorisation des problèmes et des incidents,
    vi. la gestion des problèmes et des incidents,
    vii. l'affectation des problèmes et des incidents,
    viii. la résolution et la clôture des problèmes et des incidents.

5.5 ACCESSIBILITÉ WEB

Personnes handicapées : Le GC tient à garantir l'accessibilité des personnes ayant une déficience visuelle, une déficience auditive, une mobilité réduite ou des troubles cognitifs.

Conformément aux politiques du GC en matière d'accessibilité et de convivialité, l'entrepreneur doit fournir aux clients d'autres formats de communication et de services axés sur la clientèle, selon les besoins.

L'entrepreneur doit veiller à ce que la technologie du bureau de service soit mise à niveau, puis intégrée au service à la clientèle général.

5.5.1 Accessibilité Web

Les normes sur l'accessibilité et la facilité d'emploi des sites Web sont entrées en vigueur le 1er août 2011 et le 28 septembre 2011 respectivement et ont été mises à jour le 31 mars 2013.

Les nouvelles normes remplacent la partie 2 de la Normalisation des sites Internet 2.0. Les nouvelles normes sont connues comme étant les directives pour l'accessibilité aux contenus Web (WCAG) 2.0.

Conformément à la Norme sur l'accessibilité des sites Web, l'entrepreneur devrait veiller à ce que chaque page Web du SGDSL réponde à l'ensemble des cinq exigences de conformité des Règles pour l'accessibilité des contenus Web 2.0.

Le niveau 1 de l'exigence de conformité devrait correspondre entièrement au niveau de conformité AA avant le début de toute activité opérationnelle, comme les projets pilotes et les lancements.

Le Canada évaluera la conformité du SGDSL avec les exigences de conformité des Règles pour l'accessibilité des contenus Web 2.0. Si ***La solution SGDSL*** n'arrive pas à assurer la conformité par rapport aux exigences de conformité des Règles pour l'accessibilité des contenus Web, l'entrepreneur devrait établir une stratégie et un échéancier visant à atteindre la note de conformité et les soumettre à SPAC à des fins d'approbation, et il doit prendre des mesures correctives pour atteindre la conformité.

Pendant l'évaluation de la conformité, le Canada pourrait déterminer que des éléments critiques des exigences de conformité des Règles pour l'accessibilité des contenus Web 2.0 devraient être respectés avant le début d'une activité opérationnelle. Une fois que des mesures correctives auront été appliquées pour les éléments critiques, le Canada réévaluera la situation afin de vérifier que la conformité a été atteinte.

Conformément à l'article 2.2 de la Norme sur l'accessibilité des sites Web, les exigences entourant l'accessibilité s'appliquent aux pages Web :

a) qui sont mises à la disposition du public (c.-à-d. personnes et entreprises à l'extérieur du gouvernement du Canada, comme les traducteurs et les interprètes pigistes, les membres de milieux universitaires);
b) dont le Ministère est responsable;
c) qui sont accessibles à partir des applications Web et des sites Web du GC.

De même, conformément à l'article 2.2 de la Norme sur la facilité d'emploi des sites Web, les exigences entourant la facilité d'utilisation s'appliquent à l'ensemble des applications et sites Web du GC, y compris :

a) celles qui sont mises à la disposition du public (c.-à-d. personnes et entreprises à l'extérieur du gouvernement);
b) celles dont le Ministère est responsable.

La ***solution du SGDSL*** est une application opérationnelle commerciale. Comme il s'agit d'une application mise à la disposition du public, le portail de libre-service du GC se doit d'être conforme aux exigences de la Norme sur l'accessibilité des sites Web du gouvernement du Canada. L'interface de l'utilisateur de l'application devrait satisfaire aux lignes directrices proposées dans la Norme sur l'accessibilité des sites Web, comme il est indiqué à la section 5.6 – Accessibilité des sites Web.

5.5.2 Exigences de conformité relatives aux contenus Web 2.0

a) La première exigence de conformité (niveau de conformité) définit les niveaux de conformité. L'exigence ne peut être remplie que si ce qui suit est vrai :
   i. un niveau de conformité AA est entièrement atteint;
   ii. les échecs fréquents sont évités pour tous les critères de succès applicables;
   iii. les techniques suffisantes sont appliquées de manière à satisfaire à tous les critères de succès applicables;
   iv. les techniques suffisantes propres à chaque technologie (à laquelle on fait appel) sont utilisées le cas échéant.

b) La deuxième exigence de conformité (pages complètes) définit ce qui doit être évalué dans une page Web.

c) La troisième exigence de conformité (processus complets) définit ce qui doit être évalué dans une page Web qui fait partie d'un processus.

d) La quatrième exigence de conformité (usage des technologies selon des méthodes exclusivement compatibles avec l'accessibilité) définit les façons d'utiliser les technologies auxquelles on fait appel satisfaire aux critères de succès. Elle ne peut être remplie qu'au moyen de l'utilisation des technologies suivantes :
   i. XHTML 1.0 ou version plus récente, à l'exception des éléments et attributs dépréciés; HTML 4.01 ou version plus récente, à l'exception des éléments et attributs dépréciés;
   ii. HTML 5 ou version plus récente, à l'exception des attributs obsolètes;
   iii. technologies assorties de techniques suffisantes (propres à chaque technologie) pour satisfaire à tous les critères de succès applicables.

e) La cinquième exigence de conformité (non-interférence) définit les façons d'utiliser les technologies auxquelles on ne fait pas appel pour satisfaire aux critères de succès.

Article	Norme	Adresse URL
2.2	Norme sur l'accessibilité des sites Web (mars 2013)	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601
2.2	Norme sur la facilité d'emploi des sites Web (mars 2013)	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=24227
6.1.1	Norme sur l'accessibilité des sites Web (mars 2013)	http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601

6 GESTION ET SURVEILLANCE

6.1 CONTEXTE

La Partie 6 décrit les exigences et les attentes de SPAC en matière de surveillance et de gestion de contrat. L'objectif général de SPAC est d'assurer l'adoption d'une approche uniforme en ce qui concerne la formation, les communications, la transition et les opérations à l'état stable. Le GC travaillera de concert avec l'entrepreneur afin d'établir une relation dynamique et permanente, qui est essentielle à l'atteinte des objectifs globaux liés à la ***solution du SGDSL***.

6.2 ATTENTES EN MATIÈRE DE GOUVERNANCE – MÉTHODE DE GESTION

L'entrepreneur doit travailler en collaboration avec SPAC pour élaborer un plan et une structure de gouvernance et de gestion de contrat qui satisfont aux attentes du GC ainsi qu'aux exigences du présent contrat.

6.2.1 Principes de gestion et de gouvernance

Les principes de gestion et de gouvernance doivent être établis en tenant compte des principes fondamentaux suivants :

a) Gouvernance : activités et processus destinés à protéger l'argent, les actifs, les bases de données et toutes les autres connaissances ou données afin de prévenir les pertes, l'utilisation abusive et le gaspillage.
b) Transparence : bénéfices mesurables axés sur les résultats, mesures du rendement et établissement de rapports.
c) Efficacité et rapidité : solution permettant de gérer les changements efficacement et qui se traduit par la prestation d'un service amélioré.
d) Flexibilité : solution et prestation de service novatrices axées sur la flexibilité afin de permettre un changement à plusieurs niveaux et une amélioration continue des services.

6.2.2 Principes de planification

Pour chaque plan, l'entrepreneur doit :

a) consulter SPAC et collaborer avec lui pour élaborer le plan et prendre en compte les considérations, les dépendances, les contraintes et les intervenants désignés par SPAC;
b) employer une séquence logique qui permettrait un niveau de communications adéquat pour l'ensemble des intervenants dans le but d'appuyer les intervenants de SPAC au moyen d'un processus de gestion des changements mis en place pour une transition itérative vers la ***solution du SGDSL***, ce qui nécessite la participation active du fournisseur à la gouvernance établie par SPAC pour la gestion des changements et le renvoi des enjeux aux échelons supérieurs, c.-à-d. le Comité consultatif sur les changements;
c) fournir un tableau RACI (responsabilité, approbation, consultation et information) définissant clairement les rôles et responsabilités de l'entrepreneur principal, de SPAC et de tout membre tiers concerné en ce qui a trait à l'exécution efficace du plan;
d) fournir une liste des liens de dépendance entre les tâches;
e) déterminer les phases, les jalons, les produits livrables et les étapes clés des travaux comme des tâches distinctes qui ont une date de début et de fin, une durée, qui sont confiées à un groupe de ressource(s), et dont les dépendances sont définies, de manière à ce que les dates de début et de fin des tâches soient fixées en fonction des dépendances, de la durée et des ressources;

f) définir chaque produit livrable prévu au contrat comme un jalon clé;
g) coordonner l'exécution de tâches en parallèle dans la mesure du possible;
h) fournir une liste des hypothèses de planification;
i) définir les risques, y compris :
   i. la catégorie de chaque risque;
   ii. la probabilité de chaque risque;
   iii. l'incidence si le risque se concrétise;
   iv. les mesures d'atténuation et les réponses aux risques;
   v. les mesures de surveillance;
   vi. l'affectation du risque.

6.3 PLANS DE PROJET

6.3.1 Plan de gestion de projet

L'entrepreneur doit fournir avec la réponse une ébauche de son plan de gestion de projet qui doit comprendre le plan de transition d'entrée qui été proposé dans le cadre de la présentation de sa soumission, et un plan de gestion de projet complet dans un délai de vingt (20) jours ouvrables suivant l'attribution du contrat pour examen et approbation par le chargé de projet.

Le plan de gestion de projet doit aborder de manière cohérente tous les domaines de connaissances relatifs à la gestion de projet définis dans la cinquième édition de *A Guide to the Project Management Body of Knowledge* ou dans *Projects in Controlled Environments* (PRINCE2), et il doit comprendre les éléments suivants :

a) une description sommaire de la ***solution du SGDSL***, de ses composants et de ses services;

b) un plan organisationnel qui englobe la structure de gestion et les organisations, et qui comprend des descriptions détaillées des rôles, des responsabilités et des qualifications des principaux membres du personnel de projet et des experts en la matière. Les descriptions doivent traiter des études, de la formation, de l'expérience pertinente en lien avec la fonction, du calendrier de disponibilité et de remplacement, ainsi que des responsabilités;

c) un plan de ressource(s) permettant de déterminer les niveaux de ressource(s) nécessaires pour accomplir le travail exigé en vertu du contrat et d'évaluer leur sécurité aux fins de l'exécution de la fonction appropriée, et dans lequel l'entrepreneur doit indiquer toute ressource complémentaire qui pourrait être déployée dans l'éventualité où le niveau d'effort requis est supérieur à celui qui avait été estimé initialement pour ce qui précède;

d) une structure de répartition du travail (SRT) du contrat au niveau de l'activité qui doit indiquer les liens entre l'infrastructure et tous les services connexes dans le cadre de la planification et du contrôle des coûts, du calendrier et du rendement technique, et pour laquelle les liens avec les responsabilités organisationnelles doivent être expliqués;

e) un plan de gestion et de contrôle des changements qui définit des méthodes et procédures normalisées de gestion des changements et qui vient à l'appui de la planification et du contrôle des coûts, du calendrier et du rendement technique, permettant de faire état de la situation actuelle par rapport au plan avec

exactitude ainsi que de prévoir les résultats des différentes mesures de rechange dans le cadre du projet, ce qui doit englober le travail effectué par tout sous-traitant, le cas échéant;

f) un plan de gestion des contrats de sous-traitance qui indique les relations de collaboration entre les divers sous-traitants qui participent aux travaux, décrit en détail les relations de l'entrepreneur avec les sous-traitants, présente les méthodes utilisées pour contrôler et surveiller le rendement des sous-traitants, explique de façon détaillée les méthodes de sélection des sous-traitants ainsi que les modalités de remplacement de ceux-ci, et définit les liens entre les sous-traitants et les domaines fonctionnels de l'organisation de l'entrepreneur ainsi que leur participation à des mises à jour sur l'examen de l'avancement du projet avec le chargé de projet;

g) un calendrier de projet qui indiquera clairement les activités, les événements et les liens logiques et techniques entre ceux-ci qui sont nécessaires à l'achèvement des jalons de projet clés, y compris le plan de transition d'entrée, et qui sera clairement lié à la SRT du contrat et au système de contrôle des changements;

h) un plan de gestion des communications qui devrait aborder les aspects suivants : gestion de la relation d'affaires entre SPAC et l'entrepreneur, modalités de renvoi et de collaboration avec SPAC pour résoudre les exceptions, problèmes et enjeux relatifs aux normes de service, documents de communication, besoins en matière de communication, planification conjointe, mandat proposé de tout comité conjoint (y compris la fréquence des réunions), communication des changements à venir et de leurs répercussions éventuelles sur les utilisateurs, mécanisme de rétroaction, matrice de renvoi aux échelons supérieurs et stratégie de communication;

i) un plan d'ingénierie du système qui doit assurer que les éléments de la SRT et les tâches techniques sont bien définis et contrôlés et que la conception répond exhaustivement à tous les besoins exprimés par le GC, décrire de quelle façon les exigences sont mises en correspondance avec la conception et l'offre de services prévus, présenter des preuves à l'appui du rendement et de l'adaptabilité déclarés, exposer de quelle façon les responsabilités propres aux exigences techniques seront réparties entre l'entrepreneur et le GC, et décrire le processus officiel d'examen de la conception et de la configuration, y compris les rôles des sous-traitants;

j) un plan d'assurance de la qualité (AQ) comprenant une démarche pour formuler des normes de travail et de qualité et les mettre en application, et pour passer en revue les travaux en cours. Ce plan doit en outre comprendre les renseignements suivants :
   i. une description détaillée des méthodes, des processus et des procédures de l'entrepreneur en matière d'AQ, ainsi que de leur conformité avec un système reconnu de gestion de la qualité;
   ii. les exigences en matière d'AQ pour la mise en œuvre et toutes les activités de transition, y compris les exigences en matière de rendement de base proposées;
   iii. une description de l'organisation d'AQ;
   iv. le temps qui doit être consacré par les employés du projet de SPAC pour leur participation au programme global d'AQ;
   v. les interfaces entre les fonctions d'AQ de l'entrepreneur et celles de ses sous-traitants, et la façon dont les responsabilités sont réparties;

vi. les recours procéduraux et contractuels en matière de recouvrement concernant les problèmes liés à la qualité, qui doivent être indiqués aux fins d'examen par le chargé de projet en tant que composantes du programme définitif d'AQ;

k) un plan de gestion des risques qui précise la marche à suivre pour relever les risques et en faire le suivi, isoler les événements qui déclenchent les risques, évaluer les probabilités et les incidences des risques, et établir un plan d'atténuation;

l) un plan de gestion des enjeux qui précise la marche à suivre pour relever et gérer les enjeux relatifs à la gestion des services, isoler les enjeux, évaluer les répercussions, déterminer les parties responsables et évaluer la gravité et le niveau de priorité des enjeux, et qui présente les processus de résolution;

m) un plan de gestion du rendement, y compris des mesures fondées sur des méthodes de gestion de projet bien établies telles que définies dans la cinquième édition de *A Guide to the Project Management Body of Knowledge* ou PRINCE2, afin d'assurer le suivi de la portée, du calendrier et des paramètres de coût;

n) un plan de gestion des versions relatif à la mise en œuvre de changements au service qui traite de l'infrastructure et de la documentation à l'appui comme les spécifications, les politiques, les procédures et le matériel de formation.

6.4 GESTION DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

6.4.1 Plan de gestion de la protection des renseignements personnels

L'entrepreneur doit fournir au chargé de projet, aux fins d'examen et d'acceptation, une ébauche de plan de gestion de la protection des renseignements personnels dans les quarante-cinq (45) jours ouvrables suivant l'attribution du contrat.

Au minimum, le plan de gestion de la protection des renseignements personnels doit comprendre les éléments suivants :

a) les stratégies de protection des renseignements personnels de l'entrepreneur et les méthodes précises qui seront employées pour traiter ces renseignements tout au long de leur cycle de vie;
b) la façon de veiller à ce que les renseignements personnels soient recueillis, utilisés, conservés et divulgués seulement aux fins de l'exécution des travaux prévus au contrat;
c) la façon de veiller à ce que les renseignements personnels soient accessibles uniquement aux personnes autorisées (selon le principe du besoin de connaître) aux fins de l'exécution des travaux prévus au contrat;
d) le protocole à suivre en cas d'atteinte à la vie privée et des précisions sur la façon de traiter une telle situation;
e) la façon dont l'entrepreneur veillera à ce que les exigences en matière de protection des renseignements personnels en vigueur au Canada, telles qu'énoncées dans la *Loi sur la protection des renseignements personnels*, la *Loi sur l'accès à l'information* et la *Loi sur la Bibliothèque et les Archives du Canada,* soient respectées tout au long de l'exécution des travaux et pendant toute la durée du contrat;
f) toute nouvelle mesure que l'entrepreneur mettra en oeuvre pour protéger les renseignements personnels et les documents en fonction de leur classification de sécurité;
g) la façon dont l'entrepreneur veillera à ce que tout rapport contenant des renseignements personnels soit stocké ou transmis de façon sécuritaire en fonction de sa classification de sécurité;

h) la façon dont l'entrepreneur veillera à ce que son personnel soit formé en ce qui concerne la protection des renseignements personnels et les principes connexes.

6.4.2 Mise en œuvre du plan de gestion de la protection des renseignements personnels

L'entrepreneur doit mettre en œuvre le plan de gestion de la protection des renseignements personnels (ensemble des processus, des procédures, des rôles et des responsabilités) et toute mise à jour annuelle subséquente.

L'entrepreneur doit fournir à SPAC, dans un délai de trente (30) jours ouvrables suivant une demande du chargé de projet, une preuve datant de moins de douze (12) mois (p. ex. résultats d'essais, évaluations et vérifications) attestant que le plan de gestion de la protection des renseignements personnels a été convenablement mis en œuvre, qu'il fonctionne comme prévu, qu'il produit les résultats escomptés et qu'il satisfait aux exigences en matière de protection des renseignements personnels de SPAC.

S'il est anticipé que des changements que l'entrepreneur compte apporter à l'environnement de la ***solution du SGDSL*** auront une incidence sur l'utilisation, la collecte, le traitement, la transmission, le stockage ou l'élimination de renseignements personnels, ou en tout temps à la demande du chargé de projet, l'entrepreneur doit fournir à SPAC des renseignements suffisamment détaillés sur les changements prévus aux fins de la mise à jour de l'évaluation des facteurs relatifs à la vie privée et de l'acceptation de ces changements par le chargé de projet.

L'entrepreneur doit fournir, dans les soixante (60) jours ouvrables suivant l'attribution du contrat, un guide de sensibilisation à la protection des renseignements personnels indiquant les consignes à suivre par la ou les ressource(s) de l'entrepreneur relativement à l'utilisation des renseignements personnels fournis par le GC au sujet des utilisateurs.

6.4.3 Évaluation des facteurs relatifs à la vie privée

L'entrepreneur doit fournir à SPAC l'aide demandée aux fins de la réalisation de l'évaluation des facteurs relatifs à la vie privée conformément à la Directive sur l'évaluation des facteurs relatifs à la vie privée du SCT (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308) et fournir les renseignements suivants dans les vingt (20) jours ouvrables suivant une demande de SPAC :

a) les processus opérationnels, les flux de données et les procédures qui se rapportent à l'accès à l'information ainsi qu'à la collecte, à la transmission, au traitement, au stockage et à l'élimination de celle-ci, y compris les renseignements personnels;
b) la liste des renseignements personnels utilisés par l'entrepreneur dans le cadre des travaux et les fins auxquelles chaque type de renseignement personnel est utilisé;
c) la façon dont les renseignements personnels sont communiqués et à qui ils sont communiqués;
d) une liste de tous les emplacements sécurisés où les copies papier des renseignements personnels sont conservées;
e) une liste de tous les emplacements sécurisés où les renseignements personnels sous forme lisible par machine sont conservés (p. ex. emplacement de tout serveur sur lequel une base de données renfermant des renseignements personnels est hébergée), y compris les sauvegardes de sécurité;
f) une liste de toutes les mesures prises par l'entrepreneur en vue de protéger les renseignements personnels et les documents outre celles qui sont exigées en vertu du contrat;
g) toute exigence de sécurité relative à la protection des renseignements personnels qu'il faut respecter ou recommandation connexe à laquelle il faut donner suite;

h) une explication détaillée des menaces réelles ou potentielles touchant les renseignements personnels ou les documents, accompagnée d'une évaluation des risques générés par ces menaces, et la pertinence des mesures de protection en place visant à prévenir ces risques;
i) les résultats de toute consultation réalisée dans le cadre de l'examen de l'évaluation des facteurs relatifs à la vie privée par le Commissariat à la protection de la vie privée du Canada (CPVP) avec l'approbation du CPVP.

L'entrepreneur doit mettre en œuvre les recommandations découlant de l'évaluation des facteurs relatifs à la vie privée conformément à un échéancier approuvé par SPAC.

Si des changements que l'entrepreneur compte apporter au SGDSL pourraient avoir une incidence sur l'utilisation, la collecte, le traitement, la transmission, le stockage ou l'élimination de renseignements personnels, ou en tout temps à la demande de SPAC, l'entrepreneur doit fournir à SPAC des renseignements suffisamment détaillés sur les changements prévus aux fins de la mise à jour de l'évaluation des facteurs relatifs à la vie privée et de l'acceptation de ces changements par le chargé de projet.

L'entrepreneur doit fournir une trousse de sensibilisation à la protection des renseignements personnels qui fait le survol des conditions relatives à l'utilisation, à la collecte et à la divulgation des renseignements personnels à sa ou ses ressource(s) contribuant au SGDSL.

6.5 GESTION DE LA SÉCURITÉ DES TI

6.5.1 Centre des opérations de protection des TI

L'entrepreneur doit fournir un centre des opérations de protection (COP) avant le déploiement de toute fonction dans l'environnement de production, ainsi que l'infrastructure et la ou les ressource(s) nécessaire(s) à la surveillance et à la résolution centralisées (24 heures sur 24, 7 jours sur 7, tous les jours de l'année) des incidents de sécurité liés au SGDSL.

Le COP doit :

a) coordonner les réponses aux incidents de sécurité en étroite collaboration avec SPAC;
b) offrir des services téléphoniques dans les langues officielles de SPAC (français et anglais), au choix de l'appelant, accessibles en tout temps au moyen d'un numéro de téléphone unique et réservé au COP;
c) agir comme point de contact pour les communications avec les représentants de SPAC au sujet des incidents de sécurité;
d) faire en sorte que les opérations du SGDSL ne soient pas perturbées en cas de défaillance du COP de l'entrepreneur;
e) aviser le GC dans un délai de 15 minutes si le COP n'est pas disponible, et fournir le nom de la personne-ressource avec qui le GC peut communiquer pendant la durée de l'interruption des services du COP.

Le COP doit collaborer avec le Centre de protection de l'information de SPAC dans le cadre des activités suivantes : l'intégration de processus, la surveillance, la gestion des incidents de sécurité, la réponse aux incidents de sécurité et la vérification.

Le COP doit accepter les courriels que les utilisateurs envoient à la boîte de réception fournie par l'entrepreneur. Celle-ci doit être dotée d'une fonction de réponse automatique pour accuser réception du courriel. Le personnel

du COP doit accuser réception des courriels dans les 15 minutes suivant leur réception. Le COP doit authentifier l'identité du demandeur au moyen d'un processus approuvé par SPAC.

6.5.2 Plan de sécurité des TI

Le plan de sécurité des TI doit décrire comment les exigences en matière de sécurité seront respectées, conformément au processus d'évaluation et d'autorisation de sécurité de SPAC décrit à la section 7.6 du présent EDT. L'entrepreneur doit soumettre le plan de sécurité des TI dans les quarante-cinq (45) jours suivant l'attribution du contrat. Le processus d'évaluation et d'autorisation de sécurité de SPAC est composé de trois points de contrôle en plus de l'état opérationnel, lesquels prévoient des évaluations à différents niveaux de granularité. Il est important de noter que toutes les exigences en matière de sécurité doivent faire l'objet d'un contrôle, de l'étape de la conception générale pour l'intégration et la mise à l'essai jusqu'à l'état opérationnel en bout de chaîne. De plus, puisque les contrôles dépendent de l'architecture de la solution, les contrôles effectués à chaque point de contrôle doivent être précisés par l'entrepreneur, à la satisfaction de SPAC, au cours du processus d'évaluation et d'autorisation de sécurité.

6.5.3 Plan de continuité des services et de reprise après sinistre

L'entrepreneur doit mettre à jour, à la demande de SPAC, le plan de continuité des services de TI joint à sa soumission à la lumière des commentaires formulés par le chargé de projet. L'entrepreneur doit soumettre une version révisée du plan de continuité des services et de reprise après sinistre aux fins d'acceptation.

6.5.4 Schémas de l'architecture technique

L'entrepreneur doit mettre à jour, à la demande de SPAC, les schémas de l'architecture technique joints à sa soumission à la lumière des commentaires formulés par le chargé de projet. L'entrepreneur doit soumettre une version révisée des schémas de l'architecture technique aux fins d'acceptation.

6.5.5 Approche relative à l'intégration technique

L'entrepreneur doit mettre à jour, à la demande de SPAC, l'approche relative à l'intégration jointe à sa soumission à la lumière des commentaires formulés par le chargé de projet. L'entrepreneur doit soumettre une version révisée de l'approche relative à l'intégration technique aux fins d'acceptation.

6.6 PROCESSUS D'ÉVALUATION ET D'AUTORISATION DE SÉCURITÉ DE SPAC

Le processus d'évaluation et d'autorisation de sécurité doit être exécuté dans son intégralité, et à la satisfaction de SPAC, avant le début de toute activité opérationnelle (p. ex. projet pilote, mise en service), ce qui comprend les transactions et les données de production.

Par la suite, chaque fois que des changements ou des nouvelles versions sont mis en œuvre, le processus d'évaluation et d'autorisation de sécurité doit être répété et documenté.

Afin de veiller à ce que les produits livrables liés à la sécurité soient de bonne qualité et soient développés en temps voulu, l'entrepreneur doit obtenir par contrat de sous-traitance les services d'un spécialiste de la conformité du processus d'évaluation et d'autorisation de sécurité qui agira à titre de point de contact pour les activités relatives à ce processus.

Ce spécialiste sous-traitant évaluera la conformité de l'entrepreneur aux principes et aux contrôles prévus dans le profil de contrôle de sécurité.

Afin de veiller à ce que des contrôles de sécurité adéquats soient en place, SPAC a mis au point un profil de contrôle de sécurité de base qui est abordé à l'*Appendice G*. Ce profil est basé sur les contrôles et les méthodologies du document d'orientation *ITSG-33* du Centre de la sécurité des télécommunications (CST)*, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (http://www.cse-cst.gc.ca/fr/publication/itsg-33).

SPAC détient le pouvoir décisionnel final pour ce qui est de déterminer si les preuves fournies relativement à la conformité et au ***SGDSL*** sont suffisantes dans l'éventualité où il découvre, dans le cadre de son processus d'évaluation et d'autorisation de sécurité, des risques liés à la sécurité qu'il juge inacceptables. SPAC peut exercer, à sa propre discrétion, les droits ou les recours dont il peut se prévaloir en vertu du présent contrat (y compris le droit de résilier le contrat en cas de manquement).

L'entrepreneur doit fournir un échéancier indiquant à quel moment il atteindra les points de contrôle de sécurité. Cet échéancier doit concorder avec son plan de transition d'entrée et son plan de sécurité de la TI.

6.6.1 Point de contrôle 1 du processus d'évaluation et d'autorisation de sécurité

L'entrepreneur doit réaliser les travaux suivants pour le point de contrôle 1 du processus d'évaluation et d'autorisation de sécurité :

a) conception détaillée des services de sécurité (CDSS);
b) matrice de traçabilité des exigences relatives à la sécurité.

Tous les travaux seront sujets à l'acceptation du chargé du projet.

6.6.1.1 Conception générale des services de sécurité

L'entrepreneur doit fournir une conception générale des services de sécurité qui comprend les éléments suivants :

a) un schéma général des composants qui indique clairement comment les services et les composants sont associés aux zones de sécurité du réseau et qui précise les principaux flux de données liés à la sécurité;
b) les couches de l'architecture (p. ex. communication, virtualisation, plateforme/système d'exploitation, gestion des données, intergiciels, applications opérationnelles);
c) une description des mesures de défense du périmètre de la zone du réseau;
d) une description de l'utilisation des technologies de virtualisation, s'il y a lieu;
e) une description des exigences de sécurité technique associées aux éléments de la conception générale des services, et ce, pour toutes les couches de l'architecture;
f) une description de toutes les exigences de sécurité non technique associées aux éléments organisationnels ou opérationnels généraux;
g) une description des modalités relatives à ce qui suit :

i. Contrôle d'accès	ix. Protection physique et environnementale
ii. Vérification et responsabilisation	x. Évaluation des risques
iii. Gestion de la configuration	xi. Sensibilisation et formation en matière de sécurité
iv. Planification de contingence	xii. Protection du système et des communications
v. Identification et authentification	xiii. Intégrité du système et de l'information
vi. Intervention en cas d'incident	xiv. Entretien du système
vii. Protection des médias	xv. Acquisition du système et des services
viii. Sécurité du personnel	

6.6.1.2 Matrice de traçabilité des exigences relatives à la sécurité

L'entrepreneur doit fournir à SPAC une matrice de traçabilité des exigences relatives à la sécurité qui comprend, pour chaque exigence présentée à la section 15.2 de l'*Appendice G – Sécurité et protection des renseignements personnels*, les renseignements complémentaires suivants :

a) le code d'identification de l'exigence relative au contrôle de sécurité;
b) la famille ou le nom de l'exigence relative au contrôle de sécurité;
c) le numéro de l'exigence relative au contrôle de sécurité;
d) la description du contrôle de sécurité;
e) des preuves qui indiquent comment l'exigence relative au contrôle de sécurité est traitée de manière assez détaillée dans la conception générale des services de sécurité pour permettre à SPAC de confirmer que les contrôles de sécurité respectent les exigences en matière de sécurité (veuillez consulter la section 15.2 de l'*Appendice G – Sécurité et protection des renseignements personnels* pour obtenir de plus amples renseignements);
f) la traçabilité (une référence à un élément identifiable de la conception détaillée des services de sécurité), pour permettre à SPAC de confirmer que les mesures de sécurité satisfont aux exigences en matière de sécurité.

6.6.2 Point de contrôle 2 du processus d'évaluation et d'autorisation de sécurité

Après l'acceptation des travaux associés au point de contrôle 1, l'entrepreneur doit réaliser, pour le point de contrôle 2 du processus d'évaluation et d'autorisation de sécurité, les travaux suivants (ce qui comprend leur acceptation par SPAC) :

a) conception générale des services de sécurité;
b) matrice de traçabilité des exigences relatives à la sécurité;
c) procédures de gestion du changement;
d) procédures opérationnelles de sécurité;
e) procédures d'installation des composants de sécurité.

6.6.2.1 Conception générale des services de sécurité

L'entrepreneur doit fournir une conception générale des services de sécurité qui comprend :

a) un schéma détaillé des composants (il doit s'agir d'une version approfondie du schéma général des composants);
b) des descriptions des mécanismes de sécurité technique associés aux éléments de la conception détaillée des services;
c) des descriptions des mécanismes de sécurité non technique associés aux éléments organisationnels ou opérationnels généraux;
d) une justification des principales décisions concernant la conception.

La CDSS doit être en conformité avec la conception générale des services de sécurité.

6.6.2.2 Mise à jour de la matrice de traçabilité des exigences relatives à la sécurité

L'entrepreneur doit mettre à jour la matrice de traçabilité des exigences relatives à la sécurité afin d'y inclure les renseignements complémentaires suivants pour chaque exigence de sécurité énoncée à la section 15.2 de *l'Appendice G – Sécurité et protection des renseignements personnels* :

a) le code d'identification de l'exigence relative au contrôle de sécurité;
b) la famille ou le nom de l'exigence relative au contrôle de sécurité;
c) le numéro de l'exigence relative au contrôle de sécurité;
d) la description du contrôle de sécurité;
e) des preuves qui expliquent comment l'exigence relative au contrôle de sécurité est traitée de manière assez détaillée dans la conception générale des services de sécurité pour permettre à SPAC de confirmer que les contrôles de sécurité respectent les exigences en matière de sécurité (veuillez consulter la section 15.2 de l'*Appendice G – Sécurité et protection des renseignements personnels* pour obtenir de plus amples renseignements);
f) la traçabilité (une référence à un élément identifiable de la conception générale des services) pour permettre à SPAC de confirmer que les mesures de sécurité satisfont aux exigences en matière de sécurité.

6.6.2.3 Procédures opérationnelles de sécurité

L'entrepreneur doit présenter à SPAC des procédures opérationnelles de sécurité qui comprennent les éléments suivants :

a) Pour chaque rôle d'opérateur :
    i. le calendrier des mesures liées à la sécurité à exécuter pour maintenir la posture de sécurité du SGDSL;
    ii. la façon d'utiliser les interfaces opérationnelles disponibles;
    iii. chaque mesure prévue et la façon dont l'utilisateur doit l'exécuter.

b) Rôles et responsabilités opérationnels en ce qui a trait à ce qui suit :
    i. les exigences relatives aux interactions avec les représentants de SPAC;
    ii. le calendrier et les procédures d'établissement de rapports;
    iii. le contrôle des accès;
    iv. la vérification et la responsabilisation;
    v. l'identification et l'authentification;
    vi. la protection du système et des communications;
    vii. la sensibilisation et la formation;
    viii. la gestion de la configuration;
    ix. la planification de contingence;
    x. la réponse aux incidents;
    xi. l'entretien;
    xii. la protection des médias;
    xiii. la protection physique et environnementale;
    xiv. la sécurité du personnel;
    xv. l'intégrité du système et de l'information.

6.6.2.4 Procédures d'installation des composants de sécurité

L'entrepreneur doit présenter à SPAC des renseignements détaillés sur les procédures d'installation des composants de sécurité, ce qui doit comprendre de l'information sur :

a) les procédures nécessaires aux fins de l'installation et la configuration sécurisées de la ***solution du SGDSL*** et de tous les composants connectés;
b) l'installation et la configuration de l'ensemble des solutions de sécurité technique;
c) la configuration de la sécurité des produits matériels;
d) la configuration de la sécurité des produits logiciels (commerciaux et de source ouverte).

6.6.3 Point de contrôle 3 du processus d'évaluation et d'autorisation de sécurité

Après l'acceptation des travaux associés au point de contrôle 2, l'entrepreneur doit réaliser, pour le point de contrôle 3 du processus d'évaluation et d'autorisation de sécurité, les travaux suivants (ce qui comprend leur acceptation par SPAC) :

a) un plan de vérification de l'installation des composants de sécurité;
b) un rapport de vérification de l'installation des composants de sécurité;
c) une matrice de traçabilité des exigences relatives à la sécurité actualisée mettant en correspondance la vérification de l'installation des composants de sécurité avec les exigences en matière de sécurité;
d) un plan relatif aux essais d'intégration de la sécurité;
e) un rapport relatif aux essais d'intégration de la sécurité;
f) une matrice de traçabilité des exigences relatives à la sécurité actualisée mettant en correspondance le rapport relatif aux essais d'intégration de la sécurité avec les exigences en matière de sécurité;
g) un plan d'évaluation des vulnérabilités;
h) un rapport d'évaluation des vulnérabilités;
i) une matrice de traçabilité des exigences relatives à la sécurité actualisée mettant en correspondance le rapport d'évaluation des vulnérabilités avec les exigences en matière de sécurité.

6.6.3.1 Plan de vérification de l'installation des composants de sécurité

L'entrepreneur doit présenter à SPAC, dans le cadre du plan de sécurité des TI, un plan de vérification de l'installation des composants de sécurité qui doit comprendre les éléments suivants :

a) l'approche de vérification;
b) les dispositions nécessaires pour permettre à SPAC d'assister à la vérification;
c) un aperçu des composants faisant l'objet d'une vérification de la sécurité;
d) pour chacun des composants de sécurité vérifiés :
    i. une description du scénario de vérification;
    ii. les liens de dépendance;
    iii. les résultats attendus (c.-à-d., des critères de type réussite/échec).

L'entrepreneur doit fournir à SPAC une matrice de traçabilité des exigences relatives à la sécurité actualisée qui indique, pour chaque exigence en matière de sécurité devant faire l'objet d'un essai dans le cadre du plan de vérification de l'installation des composants de sécurité, la traçabilité (référence à un élément identifiable des scénarios d'essai de vérification de l'installation des composants de sécurité).

L'entrepreneur doit effectuer la vérification de l'installation des composants de sécurité conformément au plan de vérification de l'installation des composants de sécurité accepté.

L'entrepreneur doit corriger les erreurs et omissions ayant trait à l'installation ou à la configuration relevées dans le cadre de la vérification de l'installation des composants de sécurité.

6.6.3.2 Rapport de vérification de l'installation des composants de sécurité

Le rapport de vérification de l'installation des composants de sécurité doit comprendre, pour chacun des éléments à mettre à l'essai indiqués dans le plan de vérification de l'installation des composants de sécurité :

a) les résultats attendus (c.-à-d., des critères de type réussite/échec);
b) les résultats obtenus;
c) une description des écarts et la méthode employée pour corriger ces derniers.

6.6.3.3 Plan relatif aux essais d'intégration des fonctions de sécurité

L'entrepreneur doit présenter, dans le cadre du plan de sécurité des TI, un plan relatif aux essais d'intégration des fonctions de sécurité à SPAC aux fins d'acceptation. Ce plan doit comprendre les éléments suivants :

a) les fonctions de sécurité à mettre à l'essai;
b) les dispositions nécessaires pour permettre à SPAC d'assister aux essais;
c) pour chaque fonction de sécurité ou ensemble de fonctions de sécurité, les éléments qui seront mis à l'essai, y compris :

    i. la description de chaque scénario et procédure d'essai;
    ii. les exigences environnementales;
    iii. les liens de dépendance;
    iv. les résultats attendus (c.-à-d., des critères de type réussite/échec).

L'entrepreneur doit fournir à SPAC une matrice de traçabilité des exigences relatives à la sécurité mise à jour comprenant, pour chaque exigence en matière de sécurité devant être mise à l'essai dans le cadre du plan relatif aux essais d'intégration des fonctions de sécurité, la traçabilité (une référence à un élément identifiable des scénarios d'essai relatifs aux essais d'intégration des fonctions de sécurité).

L'entrepreneur doit effectuer les essais d'intégration des fonctions de sécurité conformément au plan relatif aux essais d'intégration des fonctions de sécurité.

6.6.3.4 Rapport relatif aux essais d'intégration des fonctions de sécurité

Le rapport relatif aux essais d'intégration des fonctions de sécurité doit comprendre, pour chacun des éléments à mettre à l'essai indiqués dans le plan relatif aux essais d'intégration des fonctions de sécurité :

a) les résultats attendus (c.-à-d., des critères de type réussite/échec);
b) les résultats obtenus;
c) une description des écarts et la méthode employée pour corriger ces derniers.

6.6.3.5 Plan d'évaluation des vulnérabilités

L'entrepreneur doit présenter, dans le cadre du plan de sécurité des TI, un plan d'évaluation des vulnérabilités à SPAC aux fins d'acceptation. Ce plan doit comprendre les éléments suivants :

a) une description de la portée de l'évaluation des vulnérabilités;
b) les dispositions nécessaires pour permettre à SPAC d'assister à l'évaluation;
c) une description du processus d'évaluation des vulnérabilités;
d) une description des outils d'évaluation des vulnérabilités qui seront utilisés, y compris les versions des logiciels.

L'entrepreneur doit effectuer l'évaluation des vulnérabilités conformément au plan d'évaluation des vulnérabilités accepté.

L'entrepreneur doit apporter des correctifs et prendre les mesures correctives nécessaires dans le cadre de l'évaluation des vulnérabilités. Lorsque cela n'est pas possible (p. ex., si le temps requis pour mettre les correctifs à l'essai ou pour déterminer et tester les mesures correctives risque de grandement retarder le projet), l'entrepreneur doit créer des billets de demande de service pour tout correctif ou toute mesure corrective dont la mise en œuvre ne peut être effectuée dans le cadre de l'évaluation des vulnérabilités.

6.6.3.6 Rapport d'évaluation des vulnérabilités

Le rapport d'évaluation des vulnérabilités doit comprendre les éléments suivants :

a) une liste des essais d'évaluation des vulnérabilités qui ont été réalisés;
b) toutes les données brutes pour les résultats des essais d'évaluation des vulnérabilités dans des formats de fichiers commerciaux nommés conformément aux spécifications de SPAC;
c) pour chaque essai d'évaluation des vulnérabilités :
    i. si une vulnérabilité connue a été détectée;
    ii. une description de la vulnérabilité (le cas échéant);
    iii. une description de la mesure corrective ou du correctif qui a été mis en œuvre pour résoudre la vulnérabilité;
d) pour toute vulnérabilité non résolue :
    i. une évaluation de l'importance de la vulnérabilité;
    ii. le numéro du billet en suspens pour le correctif ou la mesure corrective;
    iii. la raison pour laquelle une mesure corrective ou un correctif n'a pas été mis en œuvre.

6.7 SERVICES DE TRANSITION

La prestation de services de transition a été divisée en différentes phases, y compris l'exigence de soutien continu. L'entrepreneur peut proposer une approche plus itérative pour la phase de la conception et la phase de la configuration. L'entrepreneur devrait présenter son approche de prestation, les besoins en ressource(s) pour l'équipe du SGDSL et le calendrier du projet dans le plan de gestion de projet.

6.7.1 Services de transition d'entrée

La ***solution du SGDSL*** doit être prête à être déployée au plus tard 12 mois après l'attribution du contrat.

6.7.1.1 Découverte et mise en correspondance des exigences fonctionnelles (feuille de route des produits et de la solution)

L'entrepreneur doit fournir au chargé de projet, dans un délai de 20 jours ouvrables suivant l'attribution du contrat, une feuille de route des produits et de la solution qui doit comprendre une liste des caractéristiques de la ***solution du SGDSL***, ainsi qu'une mise en correspondance de ces caractéristiques avec les exigences fonctionnelles définies à la *Partie 3 – Exigences fonctionnelles*.

Après le travail de découverte et d'examen des exigences fonctionnelles, l'entrepreneur mettra à jour la feuille de route des produits et de la solution en indiquant les exigences en matière de configuration et de prolongation relatives à la ***solution du SGDSL*** et soumettra le document final dans un délai de (60) jours ouvrables suivant l'attribution du contrat.

6.7.1.2 Plan de transition d'entrée

L'entrepreneur doit fournir au chargé de projet, aux fins d'examen et d'acceptation par celui-ci, un plan de transition d'entrée conformément au calendrier du projet.

Le plan de transition d'entrée doit décrire comment SPAC effectuera la transition vers la ***solution du SGDSL*** et comprendre des renseignements détaillés en ce qui concerne :

a) les activités de configuration;
b) la conversion et la migration des données;
c) la formation sur les fonctions de la solution à l'intention de l'équipe de projet du SGDSL;
d) les activités d'intégration et de mise à l'essai;
e) la connectivité avec les systèmes de SPAC tels que SIGMA;
f) la recherche fondamentale et une évaluation des exigences spécifiques liées au traitement de divers composants du SGDSL;
g) la mise à l'essai de solutions opérationnelles;
h) la livraison d'une capacité fonctionnelle;
i) la facilitation de l'intégration des clients et des utilisateurs;
j) l'intégration des données existantes;
k) l'élaboration de lignes directrices propres à la solution;
l) l'élaboration de documents pour les procédures opérationnelles;
m) l'élaboration d'une évaluation de l'état de préparation de la mise en œuvre :
    I. plan et calendrier;
    II. fiches de pointage et rapports;
    III. critères de préparation critiques ciblés et définis, qui guideront les décisions d'aller de l'avant ou non (en fonction de l'état de préparation global, pour la mise en service de tout nouveau service ou environnement de TI);
    IV. stratégie de retour en arrière.

L'entrepreneur doit travailler en collaboration avec SPAC à l'élaboration du plan de transition d'entrée.

Le plan de transition d'entrée de l'entrepreneur doit :

a) reposer sur une approche axée sur des jalons pour la gestion des activités de transition d'entrée, compte tenu de la taille et de la complexité des activités qui doivent être réalisées pour garantir une transition en douceur, laquelle approche doit diviser la ***solution du SGDSL*** en composantes fonctionnelles qui peuvent être mises en œuvre et fournies rapidement;
b) comprendre une évaluation générale de la situation actuelle de SPAC et indiquer les aspects touchés par les changements, dont les principaux processus opérationnels et les principales politiques.

6.7.1.3 Réalisation de la transition d'entrée (ou exécution)

L'entrepreneur doit :

a) exécuter le plan de transition d'entrée;
b) cerner les domaines de transition à haut risque et les répercussions connexes, élaborer des stratégies d'atténuation, recommander des mesures d'atténuation et présenter les résultats à SPAC;

c) examiner et étayer par la documentation la situation actuelle à SPAC et les processus génériques de SPAC (en se basant sur la documentation concernant les processus opérationnels existants et en animant des ateliers) et consigner les écarts entre la situation actuelle et les processus prévus par la ***solution du SGDSL***;
d) faire des suggestions liées à l'amélioration et à la refonte des processus de bout en bout actuellement utilisés dans l'ensemble de SPAC, en incluant un modèle opérationnel (ou un modèle de capacités) et un modèle de données;
e) animer des ateliers pour sensibiliser les participants aux processus prévus par la ***solution du SGDSL*** et présenter/analyser les activités d'optimisation et de refonte des processus proposées;
f) mettre au point définitivement les changements à apporter aux processus opérationnels et les documents sur les nouveaux processus nécessaires à l'harmonisation avec l'environnement configuré;
g) soumettre la version définitive des documents sur les nouveaux processus opérationnels pour le nouvel environnement de la ***solution du SGDSL*** à l'acceptation de SPAC;
h) réaliser des évaluations de l'état de préparation à la mise en œuvre et rendre compte des résultats et des recommandations chaque semaine, avant le transfert, et cerner les points ou les situations qui pourraient compromettre le succès du transfert;
i) mettre en place et appliquer des mesures correctives reposant sur des évaluations de l'état de préparation, et rendre compte des résultats à SPAC;
j) vérifier que tous les travaux, les essais, les évaluations et les mesures correctives ont été effectués, afin de s'assurer que SPAC est prêt à 100 % avant l'entrée en service, et ce, pour tous les critères de mise en œuvre;
k) formuler des recommandations sur la ligne de conduite optimale à adopter pour traiter et résoudre les problèmes propres aux intervenants;
l) élaborer une liste de vérification préalable à la mise en œuvre et des critères d'évaluation mesurables postérieurs à la mise en œuvre;
m) formuler des recommandations pour ce qui est d'aller de l'avant ou non, et préparer un document de décisions quant à la mise en œuvre, aux fins d'acceptation;
n) réaliser toutes les activités postérieures au transfert, conformément au plan de transfert, et s'assurer qu'elles sont réalisées à 100 %;
o) fournir périodiquement des rapports d'étape et des plans d'atténuation des risques.

SPAC peut examiner les produits provisoires que l'entrepreneur réalise dans le cadre du processus normal de mise en œuvre de la ***solution SGDSL***. Le cas échéant, il informera l'entrepreneur dans un délai raisonnable de son intention d'examiner de manière informelle ses produits provisoires, et lui fournira des commentaires ou des suggestions en temps opportun. Il pourrait aussi demander à l'entrepreneur de fournir des renseignements supplémentaires, notamment concernant l'identité, l'habilitation de sécurité et les qualifications du personnel responsable de certaines activités d'essai.

6.7.1.4 Essais d'intégration et du système pour la transition

L'entrepreneur doit :

a) proposer une stratégie et un plan de mise à l'essai et d'intégration visant à vérifier les exigences fonctionnelles, de rendement, de sécurité et de fiabilité qui cadrent avec les processus opérationnels, profils et rôles des utilisateurs;
b) recommander des exigences en matière d'intégration et de mise à l'essai;
c) établir, documenter et tenir à jour un plan d'intégration et de mise à l'essai qui respecte les exigences et les politiques définies;

d) effectuer tous les essais du système conformément à la stratégie et au plan de mise à l'essai approuvés;
e) fournir à SPAC des copies et/ou des résumés des résultats des essais pour confirmer que ceux-ci ont tous été réalisés et réussis.

6.7.1.5 Essais d'acceptation par les utilisateurs

SPAC effectuera des essais d'acceptation par les utilisateurs à l'égard des modules de systèmes et des caractéristiques, des fonctions et des travaux d'intégration visés par les configurations du SGDSL conformément à l'EDT, ou à la demande de SPAC. Avant de déployer des composants fonctionnels dans l'environnement de production, l'entrepreneur doit présenter chaque version principale et secondaire à SPAC afin que celui-ci procède à des essais d'acceptation par les utilisateurs. Avant qu'une version soit soumise aux fins de ces essais, l'entrepreneur doit avoir réalisé tous les essais nécessaires pour ladite version de la ***solution du SGDSL.***

Pendant la période d'essai d'acceptation par l'utilisateur, l'entrepreneur doit :

a) aider SPAC à définir la stratégie, le plan de mise à l'essai, les scénarios de mise à l'essai ainsi que les critères d'entrée et de sortie relativement aux essais d'acceptation par les utilisateurs;
b) aider SPAC à définir les catégories de gravité et les délais d'exécution;
c) définir, avec SPAC, les solutions et les outils du ***SGDSL*** à utiliser pour créer et signaler les anomalies ainsi que pour en assurer le suivi;
d) fournir à SPAC un plan de renvoi, de demande de soutien et de résolution;
e) fournir à SPAC des données et un environnement d'essai semblable à l'environnement de production pour la réalisation des essais d'acceptation par les utilisateurs;
f) faciliter la collecte de données en ce qui concerne les résultats des essais d'acceptation par les utilisateurs;
g) analyser les résultats des essais d'acceptation par les utilisateurs fournis par SPAC;
h) mettre en œuvre des mesures correctives en fonction des résultats des essais d'acceptation par les utilisateurs et des recommandations de SPAC;
i) évaluer et communiquer l'incidence globale et le risque potentiel pour les composants du système avant la mise en œuvre des changements;
j) en bout de chaîne, fournir à SPAC le rapport et les résultats complets des essais d'acceptation par les utilisateurs.

À la réception d'une version, SPAC effectuera rapidement les essais d'acceptation par les utilisateurs conformément aux scénarios et critères d'acceptation applicables, puis informera l'entrepreneur des résultats des essais. SPAC se réserve le droit d'établir les critères d'acceptation finaux pour chacune des versions.

Lorsqu'une version satisfait aux critères d'acceptation, SPAC informera l'entrepreneur par écrit qu'il accepte la version en question. Une version ne sera réputée avoir été acceptée par SPAC que lorsque l'entrepreneur recevra l'avis écrit à ce sujet. Si une version présentée à nouveau ne respecte toujours pas les critères d'acceptation, SPAC pourra demander à l'entrepreneur, sans frais supplémentaires pour SPAC, de poursuivre les travaux visant à corriger les lacunes et de prendre toutes les mesures qui s'imposent pour que le produit livrable respecte les critères d'acceptation.

Lorsqu'il présente de nouveau au chargé de projet un produit livrable qui a déjà été rejeté, l'entrepreneur doit produire un document dans lequel il décrit en termes généraux les modifications effectuées et la façon dont celles-ci viennent corriger le problème soulevé par SPAC dans l'avis de rejet. Il doit mettre l'accent sur le

respect des critères qui n'avaient pas été respectés, tels qu'énoncés dans l'avis de rejet. L'objectif est double : garantir que les besoins de SPAC sont satisfaits et accélérer le processus d'acceptation en donnant l'occasion à SPAC de se concentrer sur l'examen des modifications apportées par l'entrepreneur.

6.7.1.6 Stabilisation du programme et après-transition

L'entrepreneur doit fournir un soutien à SPAC après la transition afin de l'aider à atteindre un état stable, notamment en accomplissant les tâches suivantes :

a) résoudre tout problème de stabilisation ou problème postérieur au transfert qui a été désigné par SPAC comme hautement prioritaire dans les cinq (5) jours ouvrables suivant chaque transfert;
b) effectuer une inspection à la suite du transfert et soumettre la liste de contrôle postérieure au transfert dans les cinq (5) jours ouvrables suivant chaque transfert;
c) résoudre tout problème de stabilisation ou problème postérieur au transfert qui a été désigné par SPAC comme n'étant pas hautement prioritaire dans les quinze (15) jours ouvrables suivant chaque transfert;
d) effectuer une évaluation de stabilisation comprenant une analyse et des recommandations dans les dix (10) jours ouvrables suivant le transfert;
e) achever toutes les activités de stabilisation dans les trente (30) jours ouvrables suivant chaque transfert;
f) élaborer les communications requises destinées aux intervenants immédiatement après chaque transfert;
g) recueillir et analyser les préoccupations, les commentaires et les demandes des parties concernées, et rendre compte de cette information;
h) procéder à un examen postérieur à la transition dans les soixante (60) jours ouvrables suivant chaque transfert;
i) fournir un rapport sur les leçons apprises pendant la transition d'entrée, aux fins d'approbation par le chargé de projet, dans les quatre-vingt-dix (90) jours ouvrables suivant chaque date de mise en service, lequel rapport énoncera toutes les leçons tirées de l'exécution du plan de mise en œuvre de la transition d'entrée;
j) tenir compte des leçons apprises dans le cadre des activités de transition ultérieures (les transferts futurs, les transitions, la planification de transitions de sortie, etc.);
k) élaborer les communications nécessaires à l'intention des intervenants après la transition et obtenir l'approbation de SPAC.

6.7.1.7 Feuille de route technologique

Chaque année tout au long de la durée du contrat, l'entrepreneur doit soumettre une feuille de route technologique indiquant les versions et les mises à niveau du produit à venir au cours des deux (2) prochaines années et permettant de faire en sorte que les processus opérationnels de SPAC suivent l'évolution de la ***solution du SGDSL***.

L'entrepreneur doit permettre à un représentant du chargé de projet de participer, en tant que membre votant actif, aux comités de clients ou d'utilisateurs existants qui sollicitent de la rétroaction sur des idées relatives au développement des applications qui composent la ***solution du SGDSL***. De plus, l'entrepreneur doit solliciter chaque année auprès de SPAC des idées de mise à niveau de fonctions, et fournir une rétroaction quant à la faisabilité de les intégrer dans la feuille de route technologique et une estimation de l'échéancier et des coûts connexes.

6.7.2 Services de soutien continu

6.7.2.1 Soutien continu

L'entrepreneur doit assurer la gestion efficace du ***SGDSL*** en ce qui a trait aux activités opérationnelles quotidiennes et son environnement de production, notamment :

a) fournir des outils et des processus étayés par une documentation pour fournir le soutien nécessaire relativement au SGDSL;
b) fournir des rapports d'étape décrivant les progrès et les nouveautés en ce qui a trait au soutien continu.

Toute défaillance logicielle relevée (c.-à-d. les bogues, les fonctions qui ne s'exécutent plus comme prévu, les vulnérabilités en matière de sécurité, etc.) doit être corrigée dans un délai convenant aux deux parties. Si les parties sont incapables de convenir d'un délai et que le Canada est contraint de mettre la solution hors service, l'application sera jugée non disponible en ce qui a trait à la norme de service *5.5.4.1 – Disponibilité des applications*.

6.7.2.2 Versions, modifications et mises à jour

L'entrepreneur doit présenter à SPAC un document énonçant la politique de déploiement des versions et de mise à niveau de la solution du SGDSL dans les (60) jours ouvrables suivant l'attribution du contrat.

Une fois la **solution du SGDSL** en service, l'entrepreneur doit évaluer l'incidence des nouvelles versions de l'application ou des applications du SGDSL sur les utilisateurs et le fonctionnement des systèmes, et veiller à ce que le Canada ait la possibilité, notamment en lui donnant un préavis suffisant, de mettre à l'essai les versions, les mises à niveau ainsi que les mises à jour importantes et changements de fond au SGDSL avant leur déploiement dans l'environnement de production. L'entrepreneur doit fournir un soutien à SPAC dans le cadre des activités de mise à l'essai lorsque la **solution du SGDSL** fait l'objet de nouvelles versions, de mises à niveau ou de mises à jour, y compris en prenant les mesures suivantes :

a) conserver des matrices des versions des logiciels dans les environnements de développement, d'assurance de la qualité et de production et sur les réseaux;
b) proposer un plan d'intégration et de mise à l'essai;
c) procéder à des essais d'intégration et de sécurité pour toutes les données et tous les réseaux, en fonction des exigences définies dans le(s) plan(s) ainsi que dans les politiques et procédures de SPAC;
d) évaluer tous les nouveaux composants du système et des services et leurs mises à niveau afin de vérifier qu'ils sont conformes aux règlements, aux procédures et aux règles de sécurité de SPAC;
e) effectuer des essais d'acceptation par l'utilisateur pour toutes les modifications et mises à jour;
f) évaluer et communiquer l'incidence globale et le risque potentiel pour les composants du système.

L'entrepreneur doit prendre des mesures correctrices pour atténuer les répercussions négatives de toute version déployée sur les opérations de la ***solution du SGDSL***.

6.7.3 Entretien

L'entrepreneur doit maintenir ou rétablir le fonctionnement normal de la ***solution du SGDSL*** au moyen d'un large éventail de mesures d'entretien prévues et imprévues.

SPAC classe les mesures d'entretien dans les catégories suivantes :

1. mesures correctives;
2. mesures préventives;
3. mesures d'adaptation;

4. mesures de perfectionnement.

L'entrepreneur doit continuellement entretenir et mettre à niveau la ***solution du SGDSL***, y compris déployer de nouvelles mises à jour et versions de la solution commerciale (COTS) au fur et à mesure que ces dernières deviennent disponibles, et ce, pendant toute la durée du contrat.

L'entrepreneur doit fournir des outils de diagnostic pour surveiller le fonctionnement global de la ***solution du SGDSL*** et veiller à ce qu'elle fonctionne selon les exigences applicables en tout temps pendant l'ensemble du cycle de vie du produit, ce qui comprend la conception, le développement, la mise en œuvre, les déploiements, l'utilisation, et la mise hors service.

L'entrepreneur est chargé de la coordination ou de l'exécution des procédures et processus planifiés ou ponctuels employés aux fins de la gestion, de la mise à jour, de la surveillance et de la mise au point des opérations et du rendement de la ***solution du SGDSL*** et de son environnement.

6.7.4 Services de transition de sortie

Avant la fin du contrat ou sa résiliation, selon le cas, l'entrepreneur doit exécuter les activités nécessaires et fournir les outils et le soutien requis aux fins de la transition de la ***solution du SGDSL*** en vertu de la portée au nouveau fournisseur de services ou à la nouvelle solution (soit un nouvel entrepreneur ou un service interne de SPAC).

À cette fin, il doit notamment :

a) procéder à la migration de toutes les données du SGDSL vers le nouveau service de SPAC, y compris les renseignements nécessaires pour mettre en correspondance les données existantes du SGDSL avec le nouveau service de SPAC;
b) communiquer au nouveau fournisseur de services les leçons tirées des services de transition initiaux prévus dans la portée du présent EDT, et lui fournir les biens et la documentation relativement à ces services;
c) veiller à l'exécution toutes les activités du plan de transition des services prévues dans la portée relativement à la transition de l'infrastructure, à la transition et à la migration, à la conversion et à la migration des données, à l'intégration et à la mise à l'essai, à la gestion du changement organisationnel et au soutien à la formation, à la conformité et aux règlements, dont seul l'entrepreneur (sortant) peut être directement responsable ou qui ne peuvent être réalisées qu'avec l'appui de l'entrepreneur (sortant), en accomplissant les travaux requis et en offrant le soutien nécessaire.

6.7.4.1 Stratégie de transition de sortie

L'entrepreneur doit fournir une stratégie de transition de sortie au chargé de projet dans les douze (12) mois suivant l'attribution du contrat aux fins d'examen et d'acceptation. La stratégie de transition de sortie doit décrire dans quelle mesure la ***solution du SGDSL*** de l'entrepreneur pourra être transférée avec succès à un nouvel entrepreneur ou à un service interne de SPAC.

La stratégie de transition de sortie doit fournir de l'information sur :

a) la gestion de projet;
b) le soutien opérationnel pour la gestion du changement;
c) le soutien pour les communications et la sensibilisation;
d) la manière dont les renseignements relatifs aux structures, aux contenus, aux domaines et aux processus liés aux données ainsi qu'aux métadonnées seront transférés;

e) le soutien relatif à la conversion et à la migration de données;
f) le soutien relatif à la documentation et aux dossiers;
g) l'approche de transfert des connaissances proposée;
h) le soutien des opérations;
i) le soutien aux utilisateurs;
j) la méthode proposée en ce qui concerne les interactions avec les titulaires, y compris la présentation des fichiers de consultation dans les systèmes, les champs de données, l'explication des codes ainsi que la consultation générale en vue d'expliquer les pratiques et procédés administratifs qui ne sont pas exclusifs;
k) les éléments pertinents du rapport sur les leçons apprises pendant la transition d'entrée doivent être pris en compte;
l) la portée des services résiliés (quels services), les échéanciers, les activités, les produits livrables, les dépendances, les jalons, l'affectation des ressources et le niveau d'effort, les hypothèses, ainsi que les dépendances critiques.

6.7.4.2 Plan de transition de sortie

Dans les trois (3) mois suivant l'avis dans lequel SPAC signale son intention de procéder à une transition de sortie, l'entrepreneur doit fournir une ébauche de plan de transition de sortie au chargé de projet afin d'assurer la transition de sortie de tout service de la ***solution du SGDSL*** vers un nouveau fournisseur de services ou un nouvel entrepreneur ou vers un nouveau service de SPAC.

Ce plan de transition de sortie doit notamment :

a) cerner les risques et les problèmes liés à chaque volet de travail afin d'en assurer le suivi et de les porter à l'attention de SPAC pour examen et acceptation;
b) fournir une liste et des renseignements sur les contrats de sous-traitance et les relations connexes avec les sous-traitants;
c) fournir une liste des logiciels tiers précisant les licences, les versions, les états des mises à jour, et les frais d'entretien et de licence si de tels logiciels sont utilisés;
d) fournir une liste du personnel de l'entrepreneur autorisé à accéder aux emplacements de SPAC;
e) fournir une liste des logiciels, des scripts, des outils ou des procédures de commandement dont se sert l'entrepreneur pour exécuter les services résiliés;
f) fournir une liste des processus, des normes, des procédures, des manuels et de tous les documents de référence connexes qui sont utilisés par l'entrepreneur pour fournir les services résiliés;
g) fournir une liste de tous les projets en cours et des changements prévus pendant la période de résiliation;
h) fournir une liste des erreurs connues existantes;
i) fournir une liste des problèmes non réglés concernant les services résiliés;
j) fournir une liste complète des biens appartenant entièrement à SPAC en possession de l'entrepreneur;
k) indiquer tous les contrats et licences de tiers détenus ou exploités par l'entrepreneur selon ceux qui sont transférables (avec les coûts associés) et ceux qui ne le sont pas – pour ceux qui ne le sont pas, l'entrepreneur DOIT fournir une solution de rechange;
l) planifier l'élimination de toutes les interfaces externes de l'entrepreneur avec les systèmes de SPAC en fonction des risques et des dispositions relatives aux services;
m) fournir une liste de tout le personnel de l'entrepreneur qui a accès à la ***solution du SGDSL*** et fournir un calendrier pour que ces accès soient retirés pendant la phase de sortie appropriée.

6.7.4.3 Biens et documents liés à la transition de sortie

Afin d'aider SPAC dans le cadre de la transition de sortie et à la demande de SPAC, l'entrepreneur doit fournir les renseignements suivants dans un délai de trente (30) jours ouvrables après que SPAC lui ait signalé son intention de procéder à une transition de sortie :

a) les biens (usage exclusif et usage partagé) et les registres de biens;
b) l'état et l'historique d'entretien des biens;
c) les données et les autres renseignements de l'entrepreneur (dont les ententes de sous-traitance nécessaires à la prestation des services);
d) les renseignements sur la configuration;
e) les données stockées dans des environnements informatiques de l'entrepreneur ou d'un tiers, y compris dans des environnements fondés sur des services gérés de l'entrepreneur;
f) toutes les bases de données contenant des données appartenant à SPAC;
g) les programmes et les projets (fermés ou ouverts);
h) les bases de données de connaissances;
i) les bases de données d'incidents;
j) la documentation générale qui devrait être incluse :
    i. représentations architecturales et conceptuelles des services,
    ii. documents relatifs au logiciel (p. ex., utilisateur, administrateur autorisé),
    iii. documents récents ou mis à jour sur les procédures et les processus,
    iv. documents sur les flux et les instructions de travail,
    v. registres de gestion des services – registres des changements et des incidents,
    vi. registre des risques,
k) la documentation tactique qui devrait être incluse :
    i. rapports sur les niveaux de service,
    ii. catalogue de services,
    iii. plans de prestation de services,
    iv. registre d'incidents et de changements,
    v. calendrier de projet et de changement,
    vi. documents sur les projets prévus et en cours,
    vii. calendriers de déploiement,
    viii. documents sur la planification de la gestion du rendement et de la capacité,
    ix. plans d'innovation et de création liés aux services concernés,
    x. plans de communication et matériel sur les activités de communication prévues ou actuelles (en ligne et hors ligne);
l) la documentation stratégique qui devrait être incluse :
    i. plans relatifs aux comptes,
    ii. plans de relations stratégiques,
    iii. feuilles de route concernant la technologie et les services,
    iv. documentation sur la gouvernance et l'architecture d'entreprise.

6.8 RÉUNIONS ET RAPPORTS

6.8.1 Réunion de lancement

L'entrepreneur doit organiser une réunion de lancement avec le chargé de projet et les autorités contractantes dans la région de la capitale nationale dans un délai de (10) jours ouvrables suivant la date d'attribution du contrat.

La réunion de lancement servira, à tout le moins, à :

a) passer en revue les exigences contractuelles;
b) examiner et préciser, au besoin, les rôles et les responsabilités respectifs de l'autorité contractante, du chargé de projet et de l'entrepreneur afin d'en garantir une interprétation commune;
c) établir une relation de travail entre l'entrepreneur et les membres de l'équipe du SGDSL;
d) discuter du plan de gestion du projet et du calendrier de projet qui ont été proposés dans le cadre de la présentation de la soumission par l'entrepreneur.

L'entrepreneur doit préparer le procès-verbal de la réunion et le transmettre au chargé du projet dans les cinq (5) jours ouvrables suivant la réunion pour qu'il l'accepte. Le procès-verbal de la réunion doit comprendre le nom de tous les participants, ainsi qu'un compte rendu des discussions et des décisions prises. Toute modification devra faire l'objet d'une discussion entre le chargé de projet et l'entrepreneur.

6.8.2 Réunions d'étape hebdomadaires

L'entrepreneur doit organiser, planifier et tenir des réunions d'étape hebdomadaires avec le chargé de projet dans la région de la capitale nationale tout au long de la période de transition. Ces réunions doivent avoir pour but de renseigner le chargé de projet sur les principaux aspects du projet du SGDSL, ce qui comprend l'état du projet et l'examen du calendrier.

L'entrepreneur doit préparer le procès-verbal de la réunion et le transmettre au chargé du projet dans les cinq (5) jours ouvrables suivant la réunion pour qu'il l'accepte. Le procès-verbal de la réunion doit comprendre le nom de tous les participants, ainsi qu'un compte rendu des discussions et des décisions prises. Toute modification devra faire l'objet d'une discussion entre le chargé de projet et l'entrepreneur.

6.8.3 Rapport mensuel sur l'avancement du projet

L'entrepreneur doit préparer un rapport mensuel sur l'état d'avancement du projet et le présenter au chargé de projet aux fins d'examen et d'acceptation. Ce rapport doit comprendre les renseignements suivants :

a) l'état d'avancement général du projet;
b) l'état d'avancement par rapport au plan de gestion de projet;
c) les réalisations accomplies lors de la période en cours;
d) l'analyse du chemin critique;
e) les jalons reportés;
f) les activités prévues pour la prochaine période;
g) des données statistiques volumétriques;
h) un résumé du rendement des services;
i) une liste et une description des événements importants;
j) les risques résolus et non réglés et l'état des enjeux;
k) les résultats du sondage sur la satisfaction de la clientèle.

6.8.4 Examens semestriels concernant la gestion stratégique

L'entrepreneur doit préparer et présenter deux fois par an au chargé de projet et à la haute direction de SPAC un examen semestriel comprenant des présentations de tous les composants de la ***solution du SGDSL***. L'examen semestriel doit comprendre les éléments suivants :

a) l'état d'avancement du projet, y compris l'état des principaux problèmes;
b) les problèmes touchant actuellement la ***solution du SGDSL*** et des pistes de solution;
c) la situation relative à la gestion des risques.

6.9 SOMMAIRE DES PRODUITS LIVRABLES

Disposition de référence de l'EDT	Produit livrable	Délai
6.3.1 Plan de gestion de projet	Plan de gestion de projet :	Ébauche au moment de la soumission de la proposition et version finale dans un délai de vingt (20) jours ouvrables suivant l'attribution du contrat
6.3.1 Plan de gestion de projet	Calendrier de projet	Ébauche au moment de la soumission de la proposition Inclus et mis à jour dans la version finale du Plan de gestion de projet pour acceptation Mise à jour et examen à la réunion hebdomadaire
6.3.1 Plan de gestion de projet	Registre des risques	Ébauche au moment de la soumission de la proposition Inclus dans la version finale du Plan de gestion de projet pour acceptation Mise à jour et rapport d'étape mensuels
6.7.1.1 Découverte et examen des exigences fonctionnelles	Feuille de route des produits et de la solution	Ébauche dans un délai de (20) jours ouvrables suivant l'attribution du contrat Version finale de la Feuille de route des produits et de la solution dans un délai de (60) jours ouvrables suivant l'attribution du contrat.
6.5.4 Schémas de l'architecture technique	Schémas de l'architecture technique	Au moment de la soumission de la proposition Version finale pour acceptation conformément au plan de projet

6.5.5 Approche relative à l'intégration technique	Approche relative à l'intégration technique	Au moment de la soumission de la proposition Version finale pour acceptation conformément au plan de projet
6.12 Plan de migration des données	Plan de migration des données	Dans un délai de (60) jours ouvrables suivant l'attribution du contrat
6.7.1.4 Essais d'intégration et de système pour la transition	Plan et rapport des essais du système	Conformément au plan du projet
6.13 Formation, transfert des connaissances ET documentation	Plan de formation	Dans un délai de (45) jours ouvrables suivant l'attribution du contrat
6.13 Formation, transfert des connaissances ET documentation	Module de formation et guide de l'utilisateur	Conformément au plan de formation
6.7.1 Services de transition d'entrée	Déploiement de la solution ***SGDSL***	(12) mois suivant l'attribution du contrat
6.4.1 Plan de gestion de la protection des renseignements personnels	Plan de gestion de la protection des renseignements personnels Guide de sensibilisation à la protection des renseignements personnels	Dans un délai de quarante-cinq (45) jours ouvrables suivant l'attribution du contrat Dans un délai de soixante (60) jours suivant l'attribution du contrat
6.4.2 Mise en œuvre du plan de gestion de la protection des renseignements personnels	Plan de gestion de la protection des renseignements personnels (mise en œuvre)	Dans un délai de trente (30) jours ouvrable, sur demande
6.5.2 Plan de sécurité des TI	Plan de sécurité des TI	Dans un délai de quarante-cinq (45) jours ouvrables suivant l'attribution du contrat
6.6.1.1 Conception générale des services de sécurité	Conception générale des services de sécurité	Conformément au plan de sécurité
6.6.1.2 Matrice de traçabilité des exigences relatives à la sécurité	Matrice de traçabilité des exigences relatives à la sécurité	Conformément au plan de sécurité
6.6.3.1 Plan de vérification de l'installation des composants de sécurité	Plan de vérification de l'installation des composants de sécurité	Conformément au plan de sécurité
6.6.3.2 Rapport de vérification de l'installation des composants de sécurité	Rapport de vérification de l'installation des composants de sécurité	Conformément au plan de sécurité
6.6.3.3 Plan relatif aux essais d'intégration des fonctions de sécurité	Plan relatif aux essais d'intégration des fonctions de sécurité	Conformément au plan de sécurité
6.6.3.4 Rapport relatif aux essais d'intégration des fonctions de sécurité	Rapport relatif aux essais d'intégration des fonctions de sécurité	Conformément au plan de sécurité
6.6.3.5 Plan d'évaluation des vulnérabilités	Plan d'évaluation des vulnérabilités	Conformément au plan de sécurité

6.6.3.6 Rapport d'évaluation des vulnérabilités	Rapport d'évaluation des vulnérabilités	Conformément au plan de sécurité
6.11.1 Continuité des services	Plan de continuité des services	Ébauche jointe à la soumission Version finale conformément au plan de projet.
6.11 Plan de continuité des services et de reprise après sinistre	Résultat de l'essai des procédures de reprise	Tous les six mois
6.11.3 Plan de reprise après sinistre	Plan de reprise après sinistre	Ébauche au moment de la soumission de l'offre Finale selon le plan du projet
6.7.1.7 Feuille de route technologique	Feuille de route technologique	Ébauche jointe à la soumission Version finale conformément au calendrier
6.7.2.2 Versions, modifications et mises à jour	Versions, modifications et mises à jour	Dans un délai de (60) jours ouvrables suivant l'attribution du contrat
6.7.4.1 Stratégie de transition de sortie	Stratégie de transition de sortie	Dans les (12) mois suivant l'attribution du contrat
6.7.4.2 Plan de transition de sortie	Plan de transition de sortie	Dans les (3) mois suivant l'avis dans lequel SPAC signale son intention de procéder à une transition de sortie
6.7.4.3 Biens et documents liés à la transition de sortie	Biens et documents liés à la transition de sortie	Dans un délai de trente (30) jours ouvrables suivant l'avis d'intention de SPAC de procéder à la transition de sortie
6.8.3 Rapport mensuel sur l'avancement du projet	Rapport mensuel sur l'avancement du projet	Mensuellement
5.4.3.1 Mesure du rendement et établissement de rapports	Rapport de gestion sur le service mensuel	Mensuellement, après le début de phase de soutien continu
6.8.4 Examens semestriels concernant la gestion stratégique	Examens semestriels concernant la gestion stratégique	Deux fois par an

6.10 CADRE SUR L'ACCEPTATION DES PRODUITS LIVRABLES

6.10.1 Cadre sur l'acceptation des produits livrables

À l'exception du déploiement des exigences fonctionnelles et non fonctionnelles décrites à la *Partie 3, Exigences fonctionnelles* et à la *Partie 5, Exigences non fonctionnelles*, SPAC utilisera le cadre sur l'acceptation des produits livrables suivant pour tous les produits livrables de l'entrepreneur :

a. les produits livrables reçus par SPAC seront considérés comme des ébauches jusqu'à ce qu'ils soient acceptés par SPAC – s'ils ne sont pas acceptés par SPAC, SPAC fournira ses commentaires sur le produit livrable à l'entrepreneur dans les dix (10) jours ouvrables suivant la réception de celui-ci;
b. à la réception des commentaires par l'entrepreneur, ce dernier et SPAC peuvent convenir de les examiner conjointement avant d'en tenir compte dans le produit livrable final;

c. l'entrepreneur doit soumettre le produit livrable révisé au chargé de projet dans les dix (10) jours ouvrables suivant la réception des commentaires de SPAC ou l'examen conjoint des commentaires, selon la date la plus tardive;
d. l'entrepreneur et SPAC peuvent mutuellement accepter d'adopter des calendriers différents ou un autre processus que celui indiqué ci-dessus pour les produits livrables.

6.10.2 Acceptation ou rejet des produits livrables

SPAC se réserve le droit de rejeter les produits livrables. À la fin de la période d'examen, tel qu'indiqué à la section *6.12.1*, le chargé de projet prendra l'une ou l'autre des décisions suivantes, dont il informera l'entrepreneur par écrit : 1) accepter le produit livrable; 2) rejeter le produit livrable, sans omettre d'indiquer les motifs du rejet; 3) prolonger la période d'acceptation d'une durée convenue avec l'entrepreneur pour poursuivre l'examen.

Si SPAC rejette un produit livrable, l'entrepreneur doit apporter rapidement les correctifs nécessaires pour respecter les critères d'acceptation établis. SPAC collaborera avec l'entrepreneur pour aider ce dernier à résoudre les problèmes, notamment en lui signifiant les motifs du rejet, et ne retardera pas l'acceptation indûment.

Lorsqu'un produit livrable satisfait aux critères d'acceptation, SPAC en informera promptement l'entrepreneur par écrit. Un produit livrable ne sera réputé avoir été accepté par SPAC que lorsque l'acceptation sera signifiée par écrit.

6.10.3 Soumettre de nouveau un produit livrable rejeté

Lorsqu'il présente de nouveau à SPAC une version qui a déjà été rejetée, l'entrepreneur doit produire un document dans lequel il décrit en termes généraux les modifications effectuées par rapport à la version précédente et la façon dont ces changements viennent corriger le problème soulevé par SPAC dans l'avis de rejet. Il devrait mettre l'accent sur le respect des critères qui n'avaient pas été respectés tels qu'ils sont énoncés dans l'avis de rejet. L'objectif est double : garantir que les besoins de SPAC sont satisfaits et accélérer le processus d'acceptation en donnant l'occasion à SPAC de se concentrer sur l'examen des modifications apportées par l'entrepreneur. L'entrepreneur doit indiquer tout changement qui n'a pas été apporté ou problème qui n'a pas été résolu et expliquer pourquoi ils ne l'ont pas été.

6.10.4 Processus de soumission des produits livrables

Afin d'éviter les retards dans l'acceptation de produits livrables connexes, et les incohérences et les contradictions entre ceux-ci, l'entrepreneur devrait prendre des mesures pour éviter de soumettre plusieurs produits livrables en même temps, à moins d'indication contraire dans le contrat. Si l'entrepreneur soumet plusieurs produits livrables à la fois en dehors des dates de soumission des produits livrables indiquées dans le contrat, SPAC se réserve le droit de prendre plus de temps pour l'examen et de modifier la section *6.10.1* en conséquence.

6.11 PLAN DE CONTINUITÉ DES SERVICES ET DE REPRISE APRÈS SINISTRE

6.11.1 Contexte

L'entrepreneur doit avoir en place un plan détaillé de continuité des services et de reprise après sinistre qui précise les procédures à suivre pour assurer la continuité des services ou produits essentiels dans l'éventualité où ceux-ci sont interrompus en raison de situations comme des catastrophes naturelles, des actes terroristes et des cyberattaques, ou à cause d'installations ou d'équipements qui ont fait défaut, qui ont été endommagés ou qui ont été détruits. L'entrepreneur doit mettre ces plans et procédures à la disposition du Canada aux fins d'examen.

6.11.2 Plan de continuité des services

La planification de la continuité des services se veut un processus de planification proactif visant à s'assurer que les services ou les produits essentiels sont fournis en cas de perturbation. Les services ou les produits essentiels sont ceux qui doivent être fournis pour assurer la survie des personnes, éviter les blessures et respecter les obligations juridiques ou autres du Canada.

L'entrepreneur devrait inclure les éléments suivants dans le plan de continuité des services :

a) politique, objet et portée,
b) buts et objectifs,
c) hypothèses,
d) principaux rôles et responsabilités,
e) résultats de l'analyse des répercussions sur les opérations,
f) plans d'atténuation des risques,
g) données hors site et exigences en matière de stockage,
h) stratégie et supports de sauvegarde,
i) reprise des activités et stratégies de continuité,
j) stratégies d'exploitation de rechange,
k) état de préparation du fournisseur,
l) activation du plan et réponse universelle,
m) plan de communication et d'avis,
n) formation et exercices,
o) examen et essais,
p) tenue à jour du plan,
q) vérifications.

6.11.3 Plan de reprise après sinistre

Le plan de reprise après sinistre a pour objectif de répondre aux incidents imprévus qui pourraient avoir pour effet de menacer, de détruire ou de paralyser sévèrement la **solution du SGDSL** exploité par l'entrepreneur ou un sous-traitant. Il vise à rétablir les opérations le plus rapidement possible en minimisant les perturbations et en utilisant les données les plus récentes et les plus à jour disponibles. Il peut porter sur les dommages aux immeubles, à l'infrastructure, au matériel informatique, aux logiciels, aux données et aux ressources humaines.

L'entrepreneur doit fournir un plan de reprise après sinistre qui aborde par exemple les éléments suivants :

a) politique de reprise après sinistre, aperçu du plan et portée de celui-ci,
b) documentation et schéma de l'ensemble du réseau et du site de récupération,
c) plan de communication et d'avis,
d) survol des éléments déclencheurs qui peuvent être invoqués pour mettre en œuvre le plan,
e) liste des intervenants internes et externes pour chaque procédure visée, avec les coordonnées de ces personnes et une description de leurs rôles et responsabilités,
f) formulaires prêts à utiliser et documents employés pour aider à mettre au point définitivement le plan,
g) description de l'intervention en cas d'urgence, des opérations de sauvegarde, des procédures de récupération, y compris l'objectif de point de reprise et l'objectif de temps de reprise,
h) liste des logiciels et des systèmes qui seront utilisés pour la reprise,
i) déterminer les menaces et les vulnérabilités les plus graves et les biens les plus importants pour ***la solution du SGDSL***;
j) sommaire de la couverture d'assurance,

k) mesures proposées pour traiter les enjeux financiers et juridiques et renseignements détaillés à ce sujet,
l) description, détails et calendrier pour la vérification du plan de reprise après sinistre.

6.11.4 Exigences

SECTION DE L'EDT	Exigence
DIS_RECOV-01	L'entrepreneur doit mettre à l'essai les procédures de reprise tous les six (6) mois et fournir les résultats de cet essai à SPAC.
DIS_RECOV-02	L'entrepreneur doit viser au moins les objectifs de temps de reprise et les objectifs de point de reprise qui suivent pour le serveur central de l'entrepreneur ou du sous-traitant : a) objectif de temps de reprise – vingt-quatre (24) heures; b) objectif de point de reprise – quarante-huit (48) heures.
DIS_RECOV-03	La ***solution du SGDSL*** doit protéger toutes les données de SPAC ainsi que les registres générés ou mis à jour dans la solution contre toute perte.
DIS_RECOV-04	L'entrepreneur doit établir les procédures de reprise suivantes : a) sauvegarde, b) reprise après sinistre, y compris les scénarios de défaillance de l'installation entière, c) protection des données, d) conservation et élimination des données, e) archivage – en ligne, en pseudodirect et hors ligne (collectivement désignées comme les « procédures de reprise »).
DIS_RECOV-05	La ***solution du SGDSL*** doit garantir que l'information archivée peut être restaurée pour un accès complet dans un délai de 1 jour ouvrable.
DIS_RECOV-06	Toutes les informations recueillies par la ***solution du SGDSL***, y compris les registres de vérification, devraient être conservées dans les archives du serveur central de l'entrepreneur ou du sous-traitant.
DIS_RECOV-07	L'entrepreneur doit veiller à ce que SPAC soit toujours en mesure de récupérer, sans devoir faire appel à l'entrepreneur, les données archivées à partir des supports précisés par SPAC.
DIS_RECOV-08	L'entrepreneur doit fournir des procédures, de la documentation et de la formation en ce qui concerne la gestion des situations d'urgence sur demande de SPAC.
DIS_RECOV-09	L'entrepreneur doit fournir des outils de diagnostic des problèmes, ce qui comprend des procédures pour déterminer la cause des problèmes, en prévoir l'ampleur, et prendre des mesures pour régler toute panne matérielle ou logicielle.
DIS_RECOV-10	L'entrepreneur doit maintenir, documenter et soutenir les installations pour le stockage des données hors site et la récupération des données auprès de l'entrepreneur ou du centre de données central du sous-traitant.
DIS_RECOV-11	L'entrepreneur doit fournir de la documentation et une série de procédures en ce qui a trait à la capacité de récupération en cas d'urgence au centre de données de sauvegarde.
DIS_RECOV-12	L'entrepreneur doit fournir de la documentation sur la façon dont la main-d'œuvre sera obtenue et utilisée en cas de sinistre.
DIS_RECOV-13	L'entrepreneur doit procéder à des essais périodiques des divers aspects du plan de reprise après sinistre tel que demandé par SPAC.

SECTION DE L'EDT	Exigence
DIS_RECOV-14	L'entrepreneur doit fournir de la documentation sur la façon dont la sécurité physique du serveur central de l'entrepreneur ou du sous-traitant est assurée, y compris, en ce qui concerne le contrôle des accès, la protection contre les incendies et leur prévention, et la protection contre les défaillances électriques.
DIS_RECOV-15	L'entrepreneur doit préciser la fréquence, le calendrier et les sites des sauvegardes ainsi que le type de supports utilisés.
DIS_RECOV-16	Si l'entrepreneur a l'intention de modifier le plan de reprise après sinistre pour quelque motif que ce soit, il doit en aviser par écrit le responsable technique quinze (15) jours ouvrables avant la date de mise en œuvre des changements proposés.
DIS_RECOV-17	L'entrepreneur doit permettre à SPAC d'examiner et d'accepter le plan de reprise après sinistre et toute mise à jour subséquente.
DIS_RECOV-18	L'entrepreneur doit fournir à SPAC le plan et le calendrier des essais pour le plan de reprise après sinistre ainsi que les résultats des essais.
DIS_RECOV-19	L'entrepreneur doit fournir à SPAC un historique des incidents et des pannes imprévues et la façon dont ceux-ci ont été traités.
DIS_RECOV-20	L'entrepreneur doit fournir à SPAC les résultats passés et futurs de vérification de la planification de reprise après sinistre.

6.12 PLAN DE MIGRATION DES DONNÉES

6.12.1 Contexte

Un plan de migration des données est essentiel pour s'assurer que l'ensemble des ressources, des systèmes, des services et des applications du Bureau ont accès aux informations contenues dans la ***solution du SGDSL***. Pour ce faire, la migration des données doit être minutieusement planifiée et mise en œuvre efficacement afin d'en assurer la qualité et la fiabilité tout en perturbant les activités le moins possible.

L'entrepreneur doit télécharger les données patrimoniales dans la solution du SGDSL et aider le Bureau à transférer les données de son ancien système à la ***solution du SGDSL***. Le plan de migration des données donne un aperçu des quatre domaines clés et des sous-domaines correspondants qui devraient être abordés.

6.12.2 Migration des données

Le plan de migration des données porte sur quatre domaines clés : la planification du projet (portée, risques et contraintes), la définition (collecte des exigences), l'analyse (inspection des données sources) et la mise en œuvre (extraction, nettoyage, transformation, chargement, mise à l'essai et MISE EN SERVICE).

Le plan de migration des données doit comprendre les éléments suivants :

Planification de projet

a) élaborer un plan de projet de migration des données,
b) déterminer la portée du projet de migration,
c) établir l'équipe et les ressources du projet,
d) définir et assigner les rôles et responsabilités,
e) déterminer les risques, les contraintes, les dépendances et les hypothèses,
f) élaborer un plan d'atténuation des risques liés à la migration des données,

g) déterminer les délais, le budget et les coûts,
h) déterminer les facteurs critiques de succès,
i) élaborer un plan de communications sur la migration des données,
j) établir l'accord de service pour la migration,
k) établir les jalons et le moment de la mise en service.

Spécification

a) déterminer les attentes et les exigences opérationnelles,
b) déterminer la méthode et les exigences en matière de migration des données,
c) déterminer les exigences en matière d'extraction, de nettoyage, de transformation et de chargement des données,
d) déterminer les besoins en données des modèles conceptuels, logiques et physiques pour l'environnement cible en se basant sur les modèles de l'environnement source,
e) déterminer les règles et les contraintes de la mise en correspondance des données,
f) déterminer les exigences en matière de mise en correspondance des données,
g) déterminer les besoins en matière de capacité, de technologie et d'infrastructure de TI de l'environnement de simulation,
h) déterminer les besoins en matière de capacité, de technologie et d'infrastructure de TI de l'environnement cible,
i) déterminer les exigences en matière d'interface entre les environnements source, de simulation et cible,
j) déterminer les exigences en matière de sécurité des données et de protection des renseignements personnels,
k) déterminer les exigences en matière de correction des données et de retour en arrière,
l) déterminer les exigences pour les scripts d'extraction, de nettoyage, de transformation, de chargement et de mise à l'essai des données,
m) déterminer les exigences relatives aux essais d'intégrité des données et d'assurance de la qualité.

Analyse

a) évaluer la technologie et l'infrastructure de TI de l'environnement source,
b) déterminer le modèle conceptuel, logique et physique des données dans l'environnement source,
c) déterminer les métadonnées des données dans l'environnement source,
d) évaluer la qualité des données dans l'environnement source,
e) déterminer la source des données,
f) déterminer où les données sources sont stockées, sauvegardées et archivées,
g) déterminer l'utilisation des données, la capacité et les modèles de croissance.

Mise en œuvre

a) mise en place et configuration de l'environnement de simulation et de l'environnement cible,
b) extraction, nettoyage et mise à l'essai des données,
    1. vérifier la qualité des données de base,
    2. supprimer les données en double et s'assurer que les données sont appariées entre les différentes sources,
    3. créer et tester les scripts (requêtes de base de données et scripts de programme pour extraire les données dans un modèle logique à partir des données source et mettre à l'essai les données),
c) transformation des données,
d) essais de transformation des données,

e) chargement des données,
f) essais de chargement des données,
g) essais d'acceptation par les utilisateurs,
h) plan de retour en arrière,
i) MISE EN SERVICE.

6.13 FORMATION, TRANSFERT DES CONNAISSANCES ET DOCUMENTATION

6.13.1 Contexte

La formation, le transfert des connaissances et la documentation à l'appui fourniront à SPAC l'information, les compétences et les capacités dont il a besoin pour la transition vers la ***solution du SGDSL***, l'exécution des opérations quotidiennes et la prestation de l'expertise nécessaire aux fins de l'utilisation des caractéristiques et des fonctions de la solution pour fournir des services de traduction, de terminologie et d'interprétation au client.

L'entrepreneur doit fournir :

a) une ébauche de plan de formation au chargé de projet dans les quarante-cinq (45) jours ouvrables suivant l'attribution du contrat aux fins d'examen et d'acceptation;

b) de la formation visant l'amélioration des compétences du personnel de l'entrepreneur par l'enseignement et l'instruction (l'entrepreneur doit participer à toute formation initiale et formation continue fournies par SPAC qui lui permettront d'en apprendre davantage sur les environnements opérationnel et technique de SPAC);

c) de la formation visant à permettre au personnel de SPAC de savoir utiliser les caractéristiques et les fonctions de la ***solution du SGDSL*** et les services connexes (les méthodes d'enseignement appropriées peuvent notamment comprendre l'enseignement en classe, l'enseignement assisté par ordinateur et l'enseignement individuel);

d) l'environnement de formation, ce qui comprend la ***solution du SGDSL***, ses composants ainsi que la documentation nécessaire pour la formation du personnel de SPAC.

6.13.2 Formation et transfert des connaissances

Les services de formation et de transfert des connaissances s'entendent des activités et des produits livrables qui permettent d'assurer l'échange des connaissances entre SPAC et l'entrepreneur afin de permettre aux personnes concernées de réaliser les travaux prévus dans cet énoncé des travaux.

Le tableau suivant indique les tâches relatives à la formation et au transfert des connaissances que l'entrepreneur devrait accomplir en collaboration avec SPAC.

Activité
a) Mettre au point une stratégie de formation (tant pour avant que pour après la transition), ce qui pourrait inclure de l'encadrement, de la formation des formateurs, de la formation sur le lieu de travail, de la formation en salle de classe à l'extérieur du lieu de travail, des aide-mémoire, des guides de l'utilisateur, et des tableaux des étapes à suivre.

b)	Procéder à une vérification approfondie des niveaux de compétences des employés de SPAC en vue de déceler les lacunes dans les connaissances et de recommander les outils et la formation dont ils ont besoin pour utiliser la **solution du SGDSL** et fournir des services de soutien pour ce système.
c)	Élaborer, consigner par écrit et tenir à jour des procédures de formation et de transfert des connaissances dans les *langues officielles du Canada* qui respectent les exigences applicables et qui sont conformes aux politiques établies.
d)	Aider à la détermination des principaux intervenants, en collaboration avec l'équipe de gestion du changement, et à la création de documents de formation pour les essais d'acceptation par les utilisateurs, en collaboration avec l'équipe technique.
e)	Établir et offrir un programme de formation (dans les deux *langues officielles du Canada*) à l'intention du personnel de SPAC en ce qui concerne les services fournis par l'entrepreneur (p. ex. règles d'engagement, demandes de services).
f)	Élaborer et mettre en œuvre des procédures de transfert des connaissances qui garantiront une compréhension commune des principales composantes des environnements opérationnels et techniques.
g)	Participer à la formation sur les environnements opérationnels et techniques donnée par SPAC.
h)	Mettre à la disposition du personnel du bureau de service de la formation continue sur les environnements opérationnel et technique de SPAC telle que définie par SPAC.
i)	Évaluer, pour les différents types d'utilisateurs, les besoins initiaux en formation en vue de l'entrée en service du SGDSL, ainsi que les besoins en formation pour les nouveaux utilisateurs et les besoins en formation d'appoint par la suite.
j)	Fournir du contenu pour les modules de formation dans les deux *langues officielles du Canada* (dont la qualité est approuvée par le Bureau de la traduction) libre de droits d'auteur et de redevances pour toute modification et rediffusion par SPAC.
k)	Fournir de la formation lorsque des changements technologiques importants (tels que définis conjointement par SPAC et l'entrepreneur) sont apportés au ***SGDSL***, par exemple lorsque de nouveaux systèmes ou de nouvelles fonctions y sont ajoutés, afin de favoriser l'utilisation optimale de toutes les caractéristiques et fonctions pertinentes.
l)	Mettre à la disposition du personnel du bureau de service les documents de formation continue préparés par le SPAC en ce qui concerne ses environnements opérationnels et techniques.
m)	Fournir des locaux pour la formation des employés de SPAC.
n)	Examiner et accepter les procédures de formation et de transfert des connaissances de l'entrepreneur.
o)	Examiner et accepter le calendrier des activités de formation et de transfert des connaissances de l'entrepreneur.

6.13.3 Documentation

Les services de documentation s'entendent des activités et des produits livrables associés à l'élaboration, la révision, la tenue à jour, la reproduction et la distribution à SPAC en format papier et en format électronique de la documentation sur la ***solution du SGDSL***.

Le tableau suivant indique les tâches générales relatives à la documentation que l'entrepreneur doit accomplir en collaboration avec SPAC :

Activité

a)	Recommander des exigences et des formats en ce qui a trait à la documentation.
b)	Définir les exigences, les formats et les politiques en ce qui a trait à la documentation.
c)	Élaborer, consigner par écrit, mettre en œuvre et tenir à jour des procédures de documentation conformes aux exigences applicables et respectant les politiques établies.
d)	Gérer et mettre à jour la documentation afin d'être en mesure d'offrir le soutien nécessaire en ce qui concerne la solution, le système, les caractéristiques et les fonctions lorsque de nouvelles capacités sont déployées ou lorsque des changements sont apportés.
e)	Étayer par de la documentation les procédures d'utilisation normalisées conformément aux spécifications de SPAC (p. ex. initialisation, reprise, traitement par lots, sauvegarde).
f)	Veiller à ce que la documentation respecte la norme de qualité de SPAC en ce qui concerne les *langues officielles du Canada**.***

6.13.4 Exigences

Section de l'EDT	Exigence (OBLIGATOIRE)
TRNG-01	L'entrepreneur doit offrir à SPAC une formation sur les outils de traduction assistée par ordinateur qui comprennent, sans s'y limiter, les modules suivants : Analyseur, Éditeur, Mémoire de traduction (MT), Traduction automatique (TA) et Assurance de la qualité (AQ).
TRNG-02	L'entrepreneur doit offrir la formation dans les *langues officielles du Canada*.
TRNG-03	Le matériel de formation doit être conforme au plan de formation accepté et être disponible dans les *langues officielles du Canada*.

Section de l'EDT	Exigence (COTÉE)
TRNG-04	L'environnement de formation doit comprendre tous les flux de travaux de SPAC et doit être compatible avec un environnement de formation géré par SPAC.
TRNG-05	L'entrepreneur doit offrir à SPAC une formation sur l'utilisation appropriée des outils et procédures de vérification.
TRNG-06	L'entrepreneur doit offrir à SPAC une formation sur l'utilisation appropriée des outils et procédures d'analyse, d'établissement de rapports et de veille stratégique.
TRNG-07	L'entrepreneur doit offrir à SPAC une formation sur les caractéristiques et fonctions de gestion du flux des travaux de la ***solution du SGDSL***.
TRNG-08	L'entrepreneur doit offrir à SPAC une formation sur les caractéristiques et fonctions de gestion de la charge de travail de la ***solution du SGDSL***.
TRNG-09	L'entrepreneur doit offrir à SPAC une formation sur les caractéristiques et fonctions de sécurité de la ***solution du SGDSL***.
TRNG-10	L'entrepreneur doit offrir à SPAC une formation sur la conception, les caractéristiques et les fonctions du portail de la ***solution du SGDSL***.

Section de l'EDT	Exigence (COTÉE)
TRNG-11	L'entrepreneur doit offrir à SPAC une formation sur les processus et les procédures du bureau de service.
TRNG-12	L'entrepreneur doit fournir et mettre à jour les documents de formation au besoin ou au moment du déploiement d'une version importante, afin de tenir compte des nouvelles caractéristiques et des changements apportés.
TRNG-13	L'entrepreneur doit offrir de la formation à l'intention des utilisateurs en fonction des rôles, des droits d'accès et des permissions, y compris de la formation destinée au personnel technique sélectionné par SPAC visant expressément à leur apprendre à tirer parti des fonctions et des caractéristiques de la ***solution du SGDSL***.
TRNG-14	La formation doit être dispensée au moyen de méthodes appropriées comme l'enseignement en classe, l'enseignement assisté par ordinateur, les webinaires et l'enseignement individuel.
TRNG-15	L'entrepreneur doit offrir de la formation à l'intention des traducteurs, des terminologues, des interprètes, de toute ressource externe (FSL) et de toute autre ressource désignée de SPAC.
TRNG-16	L'entrepreneur doit offrir de la formation aux utilisateurs, à la demande de SPAC, y compris de la formation en classe et de la formation assistée par ordinateur (au cas par cas), en ce qui concerne les applications standard de son service géré et hébergé, ce qui comprend la formation à l'intention des nouveaux employés, les cours de mise à niveau et l'apprentissage de compétences spécialisées.
TRNG-17	L'entrepreneur doit offrir de la formation des formateurs pour les utilisateurs telle que définie par SPAC.
TRNG-18	L'entrepreneur doit offrir aux membres de l'équipe de projet de la formation adaptée à leurs rôles avant le déploiement de chaque nouvelle version de produit afin de favoriser l'utilisation optimale de toutes les fonctions et caractéristiques pertinentes de la ***solution du SGDSL***.
TRNG-19	L'entrepreneur doit, à la demande de SPAC, fournir des renseignements et de la formation aux utilisateurs au sujet de la solution de bout en bout afin de leur fournir le soutien dont ils ont besoin selon leurs besoins opérationnels, et ce en fonction des rôles, des droits d'accès, et des permissions.
TRNG-20	L'entrepreneur doit fournir un environnement de formation qui tient compte des mises à jour et des mises à niveau de l'environnement de production.
TRNG-21	L'entrepreneur doit fournir une formation et un transfert des connaissances qui sont adaptés aux rôles, droits d'accès et permissions des utilisateurs ainsi que de la ressource ou des ressources de SPAC.

6.14 GESTION DES CHANGEMENTS

6.14.1 Contexte

La gestion des changements vise à contrôler le cycle de vie de toutes les demandes de changement concernant les services de traduction, de terminologie et d'interprétation liées à la solution en normalisant les méthodes et

les procédures utilisées pour gérer les changements et réduire au minimum les répercussions pour les parties concernées et les interruptions de services qui pourraient avoir une incidence sur SPAC et ses clients du BT.

La gestion des changements vise différents types de changements qui peuvent être demandés et envisagés, y compris, les changements à une application, à du matériel informatique, à un logiciel, à un réseau, à l'environnement, à la documentation, de même que les changements liés à des incidents ou à des problèmes.

L'entrepreneur doit fournir des services de consultation, des services professionnels ainsi que du soutien pour aider SPAC avec la gestion des changements et l'approche à l'égard des changements.

6.14.2 Objectif

Les objectifs de la gestion du changement sont les suivants :

a) Répondre aux besoins opérationnels changeants du client en maximisant la valeur et en évitant dans mesure du possible les incidents, les perturbations et le travail à refaire.
b) Répondre aux demandes de changements opérationnels et technologiques afin d'adapter les services en fonction des besoins et objectifs opérationnels.
c) Veiller à ce que les changements soient consignés et évalués, et que les changements autorisés soient classés par ordre de priorité, planifiés, mis à l'essai, mis en œuvre, étayés par la documentation et examinés de manière contrôlée.
d) Assurer une gestion optimale des risques opérationnels dans leur ensemble :
    i. Bien qu'il convienne souvent de réduire les risques opérationnels au minimum, il est parfois approprié d'accepter sciemment des risques compte tenu des avantages potentiels.

e) Gérer les changements afin :
    i. d'optimiser l'exposition aux risques (à l'appui du profil des risques exigé par l'organisation);
    ii. de faire en sorte que toute répercussion ou perturbation soit la moins grave possible;
    iii. de réussir du premier coup;
    iv. de s'assurer que les intervenants reçoivent rapidement des communications appropriées concernant les changements, afin qu'ils soient prêts à les adopter et à fournir le soutien nécessaire.

6.14.3 Approche

Cette section décrit l'approche qui sera employée par SPAC pour gérer le cycle de vie des changements. Ce faisant, SPAC s'assurera que tous les changements proposés sont définis, évalués, examinés et approuvés afin qu'ils puissent être adéquatement mis en œuvre et communiqués à toutes les parties concernées.

L'approche suivante et les activités qui y sont définies doivent être mises en œuvre par l'entrepreneur avec la collaboration de SPAC dans le cadre de la gestion du changement :

1.0 Préparer la demande de changement
a) Créer et remplir la demande de changement visée à la section *6.14.4, Demande de changement*, en indiquant les renseignements pertinents.
b) Fournir les objectifs et l'information pour le changement et une évaluation.
c) Procéder à une analyse pour définir les risques, les coûts et les répercussions particulières des changements sur les parties concernées.

d) Examen et acceptation (parties concernées, responsable technique, entrepreneur, membre de la direction).
e) Autoriser le changement.

2.0 Planifier le changement.
a) Activités (parties concernées, responsable technique, cadre responsable)
b) Consultation de l'entrepreneur et services professionnels nécessaires pour le changement
c) Plan de communication
d) Plan et approche de retour en arrière
e) Plan et calendrier de formation

3.0 Gérer et mettre en œuvre le changement.
a) Obtenir toute ressource nécessaire et s'organiser pour gérer le changement.
b) Mettre à l'essai et valider le changement.
c) Déterminer le moment du changement.
d) Mettre en œuvre le changement.
e) Envisager le plan de retour en arrière au besoin.
4.0 Examiner, documenter et clore le changement.
a) Examen postérieur à la mise en œuvre.
b) Recueillir des commentaires afin de mesurer les résultats et l'adoption du changement souhaité.
c) Prendre des mesures correctives pour combler toute lacune.
d) Définir et mettre en œuvre des indicateurs de rendement clés et des mesures connexes.
e) Documenter le changement.
f) Clore le changement.

6.14.4 Demandes de changement

Dans le cadre de la gestion des changements, des demandes de changement seront utilisées pour communiquer les changements. Elles devraient comprendre, sans s'y limiter, les renseignements suivants :

Renseignements à fournir dans une demande de changement
a) Date et heure de la demande de changement
b) Coordonnées du demandeur

Renseignements à fournir dans une demande de changement	
c) Type de changement (standard, normal, urgent)	
i. Standard	Changements à un service ou à l'infrastructure de TI pour lesquels le processus de mise en œuvre et les risques sont connus à l'avance. Ces changements sont gérés conformément aux politiques que l'organisation de TI a déjà en place. De ce fait, ils sont les plus faciles à prioriser et mettre en œuvre et ne nécessitent généralement pas une acceptation aux fins de la gestion des risques.
ii. Normal	Changements qui doivent passer à travers les étapes du processus de changement avant d'être acceptés et mis en œuvre. S'il est déterminé que le niveau de risque associé à un changement est élevé, un comité consultatif sur les changements doit décider si ce changement sera mis en œuvre ou non.
iii. Urgent	En cas de menace ou d'erreur imprévue (p. ex. défaillance de l'infrastructure, atteinte à la sécurité, mauvais fonctionnement d'une application, incident nécessitant une intervention immédiate).
d) Catégorie de changement (essentiel, majeur, mineur)	
e) Niveau de priorité	
f) Description du changement (portée)	
g) Motif du changement	
h) Incidences du changement sur : I. les groupes ou ressource(s); II. les outils (système, application); III. les caractéristiques et fonctions.	
i) Effet de ne pas procéder au changement	
j) Avantages de procéder au changement	
k) Coût de la mise en œuvre du changement	
l) Évaluation des risques liés au changement	
m) Mise en œuvre du changement : i. Échéancier estimatif ii. Temps d'arrêt estimatif iii. Calendrier iv. Ressource(s) nécessaire(s) v. Emplacement physique	

6.14.5 Prestation

L'entrepreneur devrait présenter à SPAC des procédures de gestion des changements abordant notamment les aspects suivants :

a) la collaboration avec SPAC dans le cadre de l'exécution de la gestion des changements et de l'approche en la matière;

b) les pouvoirs de l'entrepreneur en matière de gestion des changements;
c) les rôles et responsabilités de toute ressource de l'entrepreneur au chapitre de la gestion des changements;
d) la façon dont l'entrepreneur utilisera le processus de gestion des changements et la gouvernance établie de SPAC à l'appui du développement *de la solution du SGDSL*;
e) la description du processus de gestion des changements, y compris le processus d'examen et d'approbation des changements;
f) les risques élevés cernés et leur incidence, l'élaboration de stratégies d'atténuation, la recommandation de mesures d'atténuation et la communication des résultats à SPAC;
g) l'organisation d'ateliers pour discuter des changements, les examiner, les analyser et les valider;
h) la réalisation d'évaluations de l'état de préparation et la communication des conclusions et des recommandations;
i) les mesures utilisées pour appliquer uniquement les changements autorisés;
j) l'exécution de mesures correctives reposant sur des évaluations de l'état de préparation et la communication des résultats à SPAC;
k) la formulation de recommandations sur la ligne de conduite optimale à adopter pour traiter et résoudre les problèmes des intervenants;
l) le registre de gestion des changements et de renvoi des problèmes aux échelons supérieurs;
m) la présentation périodique de rapports d'étape et de plans d'atténuation des risques conformément aux exigences de SPAC.

6.14.6 Exigences

Section de l'EDT	Exigence (OBLIGATOIRE)
CHG-MGMT-01	Si l'entrepreneur a l'intention d'apporter des changements à l'infrastructure de son centre de données (exploité par l'entrepreneur ou une tierce partie) ou à toute partie de cette infrastructure qui pourraient avoir quelque incidence que ce soit sur les services, il doit en aviser par écrit le responsable technique quinze (15) jours ouvrables avant la date de mise en œuvre des changements proposés.
CHG-MGMT-02	Tous les changements potentiels à l'infrastructure du service central de l'entrepreneur ou du sous-traitant ou à toute partie de ceux-ci pouvant avoir une incidence sur les services de la ***solution du SGDSL*** , lorsque l'entrepreneur a fourni un avis conformément à l'exigence CHG-MGMT-04, doivent être acceptés par écrit par SPAC avant d'être mis en œuvre.
CHG-MGMT-03	Les changements proposés doivent décrire les changements proposés de façon suffisamment détaillés pour permettre au responsable technique d'évaluer si ceux-ci auront ou non une incidence sur l'utilisation et le fonctionnement de la ***solution du SGDSL***. Si SPAC détermine que les changements proposés pourraient avoir une telle incidence, il en avisera l'entrepreneur par écrit. L'entrepreneur doit apporter les modifications nécessaires aux changements proposés afin de s'assurer que ceux-ci n'ont pas d'incidence sur l'utilisation ou le fonctionnement de la ***solution du SGDSL***.
CHG-MGMT-04	L'entrepreneur ne doit pas mettre en œuvre les changements proposés ou les changements proposés modifiés avant d'obtenir l'acceptation du responsable technique.

Section de l'EDT	Exigence (OBLIGATOIRE)
CHG-MGMT-05	Indépendamment de l'acceptation des changements proposés par SPAC, l'entrepreneur doit s'acquitter des obligations énoncées dans le présent énoncé des travaux.
CHG-MGMT-06	L'entrepreneur doit mettre en place un cycle de développement des produits qui permet une gestion du changement vérifiable. Il doit fournir les renseignements suivants pour chaque version de produit : ensemble des améliorations apportées, des lacunes corrigées et des problèmes connus, et versions approuvées du matériel de soutien, du système d'exploitation, du matériel de formation, de la documentation relative à l'entretien et des autres documents à employer pour la version en question.
CHG-MGMT-07	Pour chaque version de la ***solution du SGDSL*** soumise à SPAC par l'entrepreneur aux fins de mise à l'essai, l'entrepreneur doit inclure un document fournissant des renseignements détaillés sur la configuration de la version y compris, sans s'y limiter, les renseignements suivants : a) une description de la version; b) la liste de demandes de changement mises en œuvre; c) la liste des autorisations de tâche mises en œuvre; d) la liste de bogues connus; e) la version de chaque composant de la ***solution du SGDSL*** inclus dans la version, y compris tous les documents (documents de conception, spécifications, manuels, matériel de formation, etc.); f) les notes sur les essais de la version comprenant les renseignements sur les essais effectués par l'entrepreneur.
Section de l'EDT	**Exigence (COTÉE)**
CHG-MGMT-08	Un cycle de vie de développement des produits devrait être élaboré pour la ***solution du SGDSL***. Il devrait comprendre un registre vérifiable des lacunes, des mesures correctives, des essais et des vérifications de la résolution des lacunes.
CHG-MGMT-09	L'entrepreneur devrait gérer les changements et les mesures correctives se rapportant à tous les composants de la ***solution du SGDSL***.
CHG-MGMT-10	L'entrepreneur devrait évaluer les risques associés à toute modification ou mesure corrective relative à la ***solution du SGDSL*** et communiquer tous les renseignements à ce sujet à SPAC.

6.15 GESTION DES VERSIONS

6.15.1 Contexte

Les services de gestion des versions s'entendent des activités et des produits livrables qui se rapportent à la mise en œuvre de changements aux services. Ils portent notamment sur les logiciels, le matériel informatique et la documentation connexe comme les spécifications, les politiques, les procédures et le matériel de formation.

Une approche globale est adoptée pour la mise en œuvre des changements aux services afin de veiller à ce que les aspects techniques et non techniques des versions soient harmonisés et respectent toutes les exigences pertinentes.

Ces changements peuvent être mis en œuvre en déployant une combinaison de nouvelles applications, un logiciel d'infrastructure et/ou du matériel informatique neuf ou mis à niveau, ou simplement en apportant des modifications à la documentation.

Les processus et activités de gestion des versions sont interreliés et complémentaires au processus de gestion des changements et à la gestion des incidents et des problèmes.

6.15.2 Gestion des versions

Le tableau suivant indique les activités de gestion des versions qui doivent être réalisées par l'entrepreneur en collaboration avec SPAC :

Activité
a) Participer à l'élaboration du processus, des politiques et des procédures de gestion des versions en collaboration avec SPAC.
b) Étayer par de la documentation et mettre en œuvre des politiques, des procédures, des processus et des formations en matière de gestion des versions conformément au processus de gestion des versions.
c) Fournir le processus, les procédures et les politiques de gestion des versions à SPAC aux fins d'examen et d'acceptation.
d) Établir, gérer, actualiser et tenir à jour le processus, les politiques et les procédures de gestion des versions ainsi que le calendrier de déploiement pour toutes les versions prévues.
e) Élaborer, gérer, actualiser et tenir à jour le processus, les politiques et les procédures de gestion des versions ainsi que le calendrier de déploiement pour chaque version de façon coordonnée avec la gestion des changements.
f) Établir et administrer le processus de contrôle des versions aux fins de la gestion des versions des applications de SPAC.
g) Fournir le processus, les politiques et les procédures de gestion des versions ainsi que le calendrier de déploiement à SPAC aux fins d'examen et d'acceptation.
h) Élaborer pour chaque version, selon les besoins, des plans de qualité et des plans de retour en arrière et les soumettre à SPAC aux fins d'examen et d'acceptation.
i) Visiter les lieux au besoin pour évaluer le matériel et les logiciels utilisés et valider les exigences et les dépendances relatives aux trousses de versions.
j) Planifier toute ressource à mobiliser et les exigences à respecter pour la prise en charge d'une version.
k) Veiller à fournir tout logiciel, équipement ou service de soutien nécessaire pour les nouvelles versions au moment opportun.
l) Veiller à ce que tous les environnements d'essai nécessaires soient disponibles et configurés adéquatement afin que les versions puissent être mises à l'essai.
m) Planifier et tenir des réunions de gestion des versions consistant notamment à examiner les versions prévues et des résultats des changements apportés.

Activité
n) Réviser les renseignements sur la gestion des versions et les modifier en fonction des besoins de SPAC (p. ex. plan de retour en arrière, décision d'aller de l'avant ou non).
o) Fournir la documentation en ce qui concerne les versions conformément aux exigences.
p) Aviser SPAC de l'échéancier et des répercussions de la mise en œuvre des versions et fournir des communications au bureau de service.
q) Mettre en œuvre les versions conformément aux exigences en matière de gestion des changements.
r) Faire un bilan à la suite de la mise en œuvre de versions ayant nécessité la mise en application du plan de retour en arrière, et déterminer et apporter des mesures correctives ou de suivi appropriées pour réduire au minimum le risque qu'une situation semblable ne se reproduise à l'avenir.
s) Réviser et accepter les contributions aux documents de formation des utilisateurs et de communication de SPAC.
t) Planifier et gérer le processus relatif aux essais d'acceptation par les utilisateurs pour chaque version.
u) Examiner et accepter le processus et le calendrier relatif aux essais d'acceptation par les utilisateurs.
v) Fournir à SPAC des rapports de gestion des versions pour chaque version. Ces rapports doivent notamment comprendre les éléments suivants : i. dernière version de chaque composant et logiciel faisant l'objet du déploiement, ii. exigences en matière de compatibilité pour chaque composant et logiciel, iii. liste des demandes de changement visées dans la version, iv. liste des demandes de changement en attente, des problèmes connus, et des solutions de rechange disponible, v. rapports sur les essais d'acceptation par les utilisateurs pour toutes les activités de mise à l'essai.
w) Procéder à des vérifications des versions à des fins de contrôle de la qualité et en accepter les résultats.

7 SERVICES PROFESSIONNELS

7.1 SERVICES PROFESSIONNELS

Les travaux décrits dans la présente section devront faire l'objet d'une demande de SPAC par l'intermédiaire d'une autorisation de tâche, au besoin.

7.1.1 Services supplémentaires de gestion du changement et de soutien à la transformation des activités

En plus des services décrits à la section 6.7, *Services de transition*, l'entrepreneur doit, sur demande, fournir des services supplémentaires.

Catégories de services professionnels
Pour les travaux décrits dans les sections 7.2.1 *Configuration supplémentaire du système*, 7.2.2 *Migration des anciennes données*, 7.2.3 *Intégration d'un tiers* et 7.2.4 *Accès aux données* de la présente annexe.

L'entrepreneur peut être appelé à fournir les services professionnels indiqués ci-dessous, sur demande, pendant toute la durée du contrat, y compris pendant toute prolongation de ce dernier lorsque l'autorité contractante exerce les options qui y sont prévues (voir les détails dans l'Appendice D – *Responsabilités des ressources en services professionnels*).

a) Gestionnaire de projet
b) Analyste des systèmes
c) Spécialiste de la conversion de données
d) Analyste d'affaires
e) Expert-conseil en restructuration des processus opérationnels
f) Analyste de la sécurité des réseaux

7.2 TRAVAUX ADDITIONNELS

Les travaux décrits dans la présente section devront faire l'objet d'une demande de SPAC par l'intermédiaire d'une autorisation de tâche, au besoin.

7.2.1 Configuration supplémentaire du système

Conformément à la partie 5, *Exigences non fonctionnelles*, SPAC prévoit qu'il pourrait être nécessaire de modifier la solution afin de tenir compte des changements apportés à l'environnement opérationnel. Bien que l'Énoncé des travaux définisse clairement une solution souple pouvant être configurée par les ressources du Bureau de la traduction, SPAC peut demander des services supplémentaires pour appuyer les changements apportés à la configuration de la ***solution du SGDSL***.

L'entrepreneur doit fournir des services supplémentaires et proposer des ressources qualifiées et ayant de l'expérience dans la prestation de services de configuration supplémentaire du système en vue de la prestation des services.

L'entrepreneur peut être appelé à fournir les services de configuration supplémentaire du système, sur demande, pour faciliter l'analyse, la conception, l'élaboration, la configuration, la mise à l'essai et la mise en œuvre des configurations du système de base de la ***solution du SGDSL***, notamment en ce qui concerne ce qui suit :

a) gestion des demandes de services;
b) portails (client, interne et externe – gabarits et formulaires);
c) gestion des flux de travaux (tâches, règles opérationnelles, validation);
d) gestion de la charge de travail (profils des ressources, rôles, planification, ordonnancement et répartition);
e) TAO (mémoire de traduction, base de données terminologique, traduction automatique);
f) renseignements d'affaires, tableaux de bord et rapports;
g) zones du système;
h) localisation et image de marque.

7.2.2 Migration des anciennes données

L'entrepreneur doit fournir des services de migration des anciennes données et fournir des ressources ayant de l'expérience dans la migration des anciennes données en vue de la prestation des services.

Conformément à la section 4.4, *Exigences technologiques du SGDSL*, l'entrepreneur doit effectuer, permettre et appuyer, sur demande, la migration des données contenues dans les systèmes existants de SPAC et les sources de données liées à la transition dont l'énoncé des travaux ne fait pas déjà mention.

7.2.3 Intégration d'un tiers

L'entrepreneur doit fournir des services d'intégration d'un tiers et fournir des ressources qualifiées et ayant de l'expérience dans la prestation de services d'intégration d'un tiers en vue de la prestation des services.

Conformément à la partie 4, *Exigences techniques*, l'entrepreneur doit effectuer, permettre et appuyer, sur demande, l'intégration à des systèmes et à des sources de données supplémentaires de tiers dont l'énoncé des travaux ne fait pas déjà mention.

7.2.4 Accès aux données

L'entrepreneur doit fournir sur demande une copie des données de la ***solution du SGDSL*** de SPAC dans un format qui n'a pas encore été défini par SPAC. La copie des données sera conservée au Canada. Les exigences, comme les types de données, les exigences de sécurité, le format de fichier, la fréquence des mises à jour delta et l'emplacement des données stockées, seront déterminées à une date ultérieure. Le format des données ne doit pas dévier du format d'origine et ne doit pas être converti en format propriétaire puisque le Canada doit être en mesure d'avoir accès aux données en tout temps.

8 APPENDICE A – GLOSSAIRE

GLOSSAIRE DES TERMES

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

A

Accès à distance : Accès au SGDSL par l'intermédiaire d'un réseau externe (p. ex., Internet).

Accès non autorisé : Fait pour une entité d'accéder au système sans en avoir l'autorisation afin de commettre une autre infraction criminelle, comme la destruction de renseignements contenus dans le système (p. ex., infiltration, compromission, piratage, augmentation de privilèges et accès non autorisé à des privilèges).

Accès sécurisé : Capacité à donner ou à refuser l'accès d'un utilisateur aux ressources contenues dans la solution du SGDSL.

Accord sur les niveaux de service : Décrit les indicateurs ou les paramètres de rendement et les valeurs minimales que le fournisseur s'engage à fournir. L'accord inclut souvent un temps ou un pourcentage de disponibilité (99,9 % ou 99,99 %) pour certaines fonctions clés, la prestation du service (ou la qualité du service), le délai de réponse aux incidents et aux problèmes, le délai de réponse à certaines demandes de service, et possiblement d'autres paramètres de service, comme le délai de déploiement des correctifs, de remplacement des pièces, de notification des incidents, etc.

Adaptabilité : Capacité d'un système, d'un réseau ou d'un processus à gérer une quantité variable de travail de façon compétente, ou capacité de cet élément à être développé pour s'adapter à la croissance. Il est ainsi possible d'accroître la capacité du matériel informatique et des logiciels au fil du temps, plutôt que de les remplacer. Un réseau adaptable devrait être en mesure de prendre en charge des connexions supplémentaires sans que le transfert de données ralentisse. Dans un cas comme dans l'autre, le matériel adaptable peut être développé de façon à répondre à la demande croissante. Même si tout le matériel informatique et tous les logiciels ont certaines limites, l'équipement et les logiciels adaptables présentent un avantage à long terme par rapport à ceux qui ne peuvent pas être développés au fil du temps.

Adaptabilité verticale : Peut essentiellement redimensionner votre serveur sans modifier votre code. Il s'agit de la capacité d'accroître la capacité du matériel ou des logiciels existants en ajoutant des ressources [p. ex., la mémoire vive, l'unité centrale de traitement (UCT) ou le disque dur externe]. L'adaptabilité verticale est limitée à la taille du serveur.

Aide offerte/Aide reçue : Nombre calculé de jour-interprète. Les interprètes des services d'interprétation parlementaire sont parfois affectés aux services d'interprétation de conférences et vice-versa. Ce rapport est nécessaire pour les considérations d'ordre budgétaire et la production de rapports.

Analyse : Terme couramment utilisé dans les entreprises pour décrire un produit (rapport analytique, analyse ou modèle statistique, ou tout autre rapport ou un résumé des données) généré pour répondre à une seule question opérationnelle précise.

Analyse des causes fondamentales : Décrit une vaste gamme d'approches, d'outils et de techniques utilisés pour découvrir les causes des problèmes.

Analyse des répercussions sur les opérations (ARO) : Une analyse qui définit les répercussions de perturbations sur une organisation en plus de définir et de classer par ordre de priorité les services essentiels et les activités à maintenir.

Analytique : L'analytique exige souvent l'examen des données historiques en vue d'observer les tendances possibles, d'évaluer les répercussions de certains événements ou décisions ou de mesurer le rendement d'un outil, d'une ressource, d'une tâche ou d'une *activité* quelconque. L'analytique a pour but d'améliorer le processus opérationnel pendant l'acquisition de connaissances qui peuvent servir à apporter des améliorations ou des changements.

Annexe : Une annexe est un document distinct qui offre des renseignements supplémentaires qui s'ajoutent à ceux contenus dans le document principal.

Aperçu : Aperçu des données à un moment précis dans le temps.

Appendice : Un appendice contient des données qui ne peuvent pas être insérées dans le document principal, et comporte des renvois à la copie ou au fichier initial.

Approbateur : Rôle attribué au cas par cas, afin de définir un niveau d'approbation supplémentaire tout au long du processus d'approbation.

Architecte de la gestion de l'information (GI) : L'architecte de la GI fournit des conseils sur les pratiques de gestion de l'information et l'architecture des données et est responsable de la préparation et de l'entretien des modèles de données d'entreprise. L'architecte de la GI fournit un soutien aux entreprises et au STI en analysant les données et en trouvant des solutions aux problèmes liés aux sujets suivants : modélisation et conception des données, intégration, gestion des données de référence, gestion des métadonnées, relations entre les données, qualité des données, transformation des données, reproduction des données et sécurité et protection des données, etc.

Architecture axée sur le service (SOA) : Style de conception de logiciel selon lequel les services sont fournis aux autres composantes au moyen d'éléments d'application, selon un protocole de communication sur un réseau.

Architecture de données : Ensemble des modèles, des politiques, des règles et des normes régissant la collecte de données ainsi que les méthodes visant à enregistrer, à organiser, à intégrer et à appliquer les données dans les systèmes de données et les organisations.

Assurance de la qualité : Système d'activités dont le but est de garantir que le contrôle de la qualité est effectué de façon efficace. Pour un bien ou un service particulier, cela comprend la vérification, les audits et l'évaluation des facteurs de qualité qui ont une incidence sur la spécification, la production, l'inspection et la distribution.

Attribution d'un contrat : Méthode utilisée dans le cadre du processus d'approvisionnement afin d'évaluer les propositions (offres des soumissionnaires) et d'attribuer le contrat pertinent. Habituellement à cette étape, l'admissibilité des propositions a été confirmée et il ne reste qu'à choisir la meilleure des propositions.

Authentification : Processus visant à vérifier l'identité numérique de l'expéditeur d'une communication par réseau.

Autorisation de tâches : Document administratif grâce auquel un utilisateur autorise un entrepreneur à effectuer les travaux « selon la demande », conformément aux modalités d'un contrat assorti d'une autorisation de tâches.

Avis : Annonce électronique qui demande des biens ou des services, indique qu'une demande de soumissions a été mise à jour ou modifiée, ou annonce l'attribution d'un contrat.

B

Base de connaissances : Répertoire de gestion des connaissances qui permet de recueillir, d'organiser, d'extraire et d'échanger des renseignements actuels ou antérieurs. La base procure la connaissance ou la justification nécessaire à la prise de décisions éclairées.

Bibliothèque d'infrastructure de la technologie de l'information (BITI) : Un ensemble de pratiques en matière de gestion des services de TI (GSTI) axé sur l'harmonisation des services aux besoins de l'organisation. Dans sa présentation actuelle (connue sous le nom de ITIL 2011), la BITI est publiée sous forme d'une série de cinq volumes principaux, et chacun d'eux porte sur une différente étape du cycle de vie de la GSTI.

C

Cadre dynamique d'évaluation de la qualité de TAUS (CDEQ TAUS) : Permet l'exécution d'analyses comparatives et fournit un cadre des modèles d'évaluation de la qualité de la traduction qui conviennent le mieux selon le type de contenu.

Catégories de correspondance de traductions :

Répétitions – Cette ligne affiche le nombre et/ou le pourcentage de mots, de caractères ou de segments qui sont des répétitions de mots comptés précédemment.

Correspondance de contexte – Cette ligne affiche le nombre et/ou le pourcentage de mots, de caractères ou de segments pour lesquels une correspondance de contexte a été trouvée dans la mémoire de traduction.

Correspondance exacte (100 %) – Cette ligne affiche le nombre et/ou le pourcentage de mots, de caractères ou de segments pour lesquels une correspondance exacte (100 %) a été trouvée.

Correspondance floue (95 % - 99 %), (85 % - 94 %), (75 % - 84 %), (50 % - 74 %) – Ces lignes affichent le nombre et/ou le pourcentage de mots, de caractères ou de segments qui ont été traduits avec une correspondance moins que parfaite (100 %) de la mémoire de traduction. Le degré de concordance est indiqué par le pourcentage.

Correspondance floue interne (95 % - 99 %), (85 % - 94 %), (75 % - 84 %), (50 % - 74 %) – Ces lignes affichent l'avantage supplémentaire que le traducteur peut obtenir en traduisant interactivement le document avec une mémoire de traduction. Voir Exécuter l'analyse de floue interne pour plus de détails.

Nouveau – Cette ligne affiche le nombre et/ou le pourcentage de mots, de caractères ou de segments pour lesquels aucune correspondance n'a été trouvée dans la mémoire de traduction.

Centre de données : Installation utilisée pour héberger des systèmes informatiques et des composantes connexes, comme des systèmes de télécommunication et de stockage.

Centre de données de niveau 1 – Chemin de distribution unique non redondant desservant l'équipement de TI. Composants de capacité non redondants. Infrastructure de base du site avec une disponibilité prévue de 99,671 %. Utilisé par des petites entreprises avec 99,671 % de temps de fonctionnement, pas de redondance et 28,8 heures de temps d'arrêt par an.

Centre de données de niveau 2 – Satisfait ou dépasse toutes les exigences du niveau 1. Composantes redondantes de la capacité de l'infrastructure du site avec une disponibilité prévue de 99,741 %. Redondance partielle de l'alimentation et du refroidissement, 22 heures d'arrêt par an.

Centre de données de niveau 3 – Satisfait ou dépasse toutes les exigences des niveaux 1 et 2. Chemins de distribution multiples indépendants desservant l'équipement de TI. Tout l'équipement de TI doit être à double alimentation et entièrement compatible avec la topologie de l'architecture d'un site. L'infrastructure du site doit pouvoir être entretenue simultanément avec une disponibilité prévue de 99,982 %. Utilisé par les grandes entreprises avec au plus 1,6 heure de temps d'arrêt par an et une tolérance N+1 aux pannes fournissant au moins 72 heures de protection contre les pannes de courant.

Centre de données de niveau 4 – Satisfait ou dépasse toutes les exigences des niveaux 1, 2 et 3. Tout l'équipement de refroidissement est à double alimentation, y compris les refroidisseurs et les systèmes de chauffage, de ventilation et de climatisation (CVC). Infrastructure de site tolérante aux pannes avec des installations de stockage et de distribution d'électricité avec une disponibilité prévue de 99,995 %. Il est utilisé par les sociétés et offre une infrastructure entièrement redondante 2N+1 (la principale différence entre les centres de données de niveau 3 et de niveau 4), 96 heures de protection contre les pannes de courant, 26,3 minutes de temps d'arrêt annuel.

Centre de la sécurité des télécommunications (CSTC) : Le CSTC a comme mandat d'acquérir et de fournir des renseignements électromagnétiques étrangers et d'offrir des conseils, des directives et des services pour assurer la protection des renseignements électroniques et de l'infrastructure des renseignements du gouvernement du Canada.

Centre de protection de l'information (CPI) : Point de contact du gouvernement du Canada pour les incidents de sécurité.

Centre des opérations de sécurité (COS) : Le Centre des opérations de sécurité est responsable de surveiller, de prévenir, de détecter et d'évaluer les menaces à la cybersécurité qui peuvent avoir des répercussions sur le système et l'information qu'il contient et d'intervenir adéquatement.

Client : Bureau de la traduction de SPAC.

Comité consultatif sur les changements (CCC) : Un groupe de personnes constitué officiellement pour représenter les fonctions de prestation de services et de soutien et qui est responsable d'évaluer, de planifier et d'autoriser les changements à apporter à l'environnement TI.

Comité pour l'évaluation de la conformité (CASCO) : Le CASCO est le Comité ISO qui se penche sur les questions touchant l'évaluation de la conformité. Il élabore des politiques et publie des normes liées à l'évaluation de la conformité, mais n'exécute pas les activités liées à l'évaluation de la conformité.

Commande : Achat fait à partir d'une méthode d'approvisionnement conformément aux modalités applicables.

Commercial sur étagère (COTS) : Décrit les logiciels et le matériel prêts à l'usage qui ne nécessitent aucune personnalisation avant l'installation.

Commissariat à la protection de la vie privée du Canada (CPVP) : Le CPVP offre des conseils et de l'information aux personnes sur la façon de protéger leurs renseignements personnels. Il est également chargé d'appliquer deux lois fédérales sur la protection de la vie privée qui établissent les règles que les institutions fédérales et certaines entreprises doivent suivre dans le traitement des renseignements personnels.

Commission électrotechnique internationale (CEI) : Une organisation internationale de normalisation qui prépare et publie des normes internationales pour toutes les technologies de l'électricité, de l'électronique et des domaines connexes – collectivement appelées électrotechnologie.

Common Event Format (CEF) : Le CEF est une norme de gestion de l'ouverture des fichiers journaux qui améliore l'interopérationalité des renseignements liés à la sécurité au moyen de différents périphériques de réseau et applications. Le CEF permet aux clients d'utiliser un journal d'événement habituel pour faciliter la collecte et le regroupement des données au moyen d'un système de gestion d'entreprise.

Conception détaillée des services de sécurité (CDSS) : La CDSS est une version plus détaillée de la conception générale des services de sécurité et doit comprendre ce qui suit :

a) un schéma détaillé des composants (il doit s'agir d'une version approfondie du schéma général des composants);

b) une description de la répartition des mécanismes de sécurité technique au sein des éléments de la conception détaillée des services;

c) la description de l'association des mécanismes de sécurité non technique aux éléments de la conception générale qui concernent l'organisation ou les opérations;

d) une justification des principales décisions concernant la conception.

Conception générale des services de sécurité (CGSS) : La CGSS comprend :

a) un schéma général des composants qui illustre clairement la répartition des services et des composants dans les zones de sécurité du réseau et qui établit les principaux flux de données liés à la sécurité;
b) les couches de l'architecture (p. ex., communication, virtualisation, plateforme/système d'exploitation, gestion des données, intergiciels, applications opérationnelles;
c) une description des mesures de défense du périmètre de la zone du réseau;
d) une description de l'utilisation des technologies de virtualisation, s'il y a lieu;
e) une description de la répartition de l'ensemble des exigences de sécurité technique dans les éléments de la conception générale des services, et ce, pour toutes les couches de l'architecture;
f) une description de la répartition de l'ensemble des exigences de sécurité non technique au sein des éléments organisationnels ou opérationnels généraux;
g) une description de l'approche relativement à :

i.	le contrôle d'accès	iv.	la protection physique et environnementale
ii.	la vérification et la responsabilité	v.	l'évaluation des risques
iii.	la gestion de la configuration	vi.	la sensibilisation et la formation sur la sécurité
iv.	la planification d'urgence	vii.	la protection du système et des communications
v.	l'identification et l'authentification	viii.	l'intégrité du système et de l'information
vi.	l'intervention en cas d'incident	ix.	l'entretien du système
vii.	la protection des médias	x.	l'acquisition de systèmes et de services
viii.	la sécurité du personnel		

Concordancier : Programme informatique qui établit automatiquement des concordances. Les résultats d'un concordancier peuvent alimenter un système de mémoire de traduction pour la traduction assistée par ordinateur (TAO), ou servir de première étape dans une traduction automatique (TA). Les concordanciers sont également utilisés en linguistique de corpus pour récupérer des listes de données linguistiques triées par ordre alphabétique ou autre à partir du corpus en question, que le linguiste de corpus analyse par la suite.

Connectivité : S'entend des appareils en communication – ce qui rend possible le transport ou la réception de données. Toutefois, ce système est davantage axé sur la collecte de renseignements plutôt que sur l'intégration des renseignements.

Contrôle d'accès : Contrôles de sécurité permettant d'autoriser ou d'interdire l'accès des ressources ***au*** SGDSL.

Contrôle de la qualité : Gamme d'activités dont le but est de vérifier que le produit ou le service offert est conforme aux exigences en matière de qualité.

Corpus : Ensemble de textes de la langue écrite (ou parlée) présentés sous forme électronique qui démontre la façon dont une langue est utilisée dans des situations réelles.

D

Débit : Exécution de tâches par un service ou un appareil informatique au cours d'une période spécifique. Pour les systèmes de traitement des transactions, il est normalement mesuré en transactions par seconde. Pour les systèmes traitant des données en vrac, comme les serveurs audio ou vidéo, il s'agit d'un débit de données (p. ex., mégaoctets par seconde). Le débit d'un serveur Web est souvent exprimé en nombre d'utilisateurs pris en charge – bien que cela dépende clairement du niveau d'activité des utilisateurs, qui est difficile à mesurer de manière cohérente.

Délai de réponse (millisecondes – réseau, serveur) : Mesure représentant le temps qu'il faut à une charge de travail pour placer une demande de travail sur le réseau, le serveur ou l'environnement virtuel et pour que le réseau, le serveur ou l'environnement virtuel exécute la demande.

Délégué : Toute personne à qui est accordée l'autorisation d'agir au nom d'un autre utilisateur dans le but d'exécuter ou d'approuver un ensemble défini de tâches.

Demande de changement (DC) : Document contenant une demande de modification d'un système; il est de grande importance pour le processus de gestion du changement.

Demande de propositions (DP) : Forme d'appel de soumissions utilisée lorsque le choix d'un fournisseur ne peut se baser uniquement sur le prix le plus bas. Une DP est utilisée pour obtenir la solution la plus rentable, d'après les critères d'évaluation qui y sont définis.

Directives pour l'accessibilité aux contenus Web (WCAG) : Cette directive définit comment rendre le contenu Web plus accessible aux personnes ayant un handicap. L'accessibilité concerne une vaste gamme de handicaps, y compris les handicaps visuels, auditifs, physiques, de la parole, de l'apprentissage, du langage et neurologiques.

Disponibilité : Réseau, stockage, serveur, ANS - min 99,95. Cette mesure est le pourcentage de temps pendant lequel un service ou un système est disponible. Il s'agit du rapport entre la durée de fonctionnement d'un système ou d'un composant et la durée totale de fonctionnement requise ou prévue. Cela peut être exprimé en proportion directe (p. ex., 9/10 ou 0,9) ou en pourcentage (p. ex., 90 %). Elle peut également être exprimée en termes de temps d'arrêt moyen par semaine, mois ou année ou en temps d'arrêt total pour une semaine, un

mois ou une année donné. Parfois, la disponibilité est exprimée en termes qualitatifs, ce qui indique dans quelle mesure un système peut continuer à fonctionner lorsqu'une composante ou un ensemble de composantes importantes diminue.

Disponibilité de l'application : Le pourcentage du temps où la ***solution du SGDSL*** est disponible dans le cadre des activités opérationnelles habituelles.

Document (DOC) : Document ou un fichier texte ASCII avec des codes de formatage de texte dans le texte; utilisé par de nombreux logiciels de traitement de texte.

Document Word Perfect (WPD) : Format de fichier de document texte.

Dossier : Information créée, reçue et conservée sous n'importe quel format à titre de preuve ou à titre informatif par une organisation ou une personne dans l'exercice de ses obligations juridiques ou à des fins professionnelles.

Droits d'accès : Façon de contrôler, de réglementer ou de restreindre l'accès au système à un utilisateur en fonction des rôles et des droits de ce dernier.

E

Éditeur : L'éditeur est la ***solution*** frontale ***du SGDSL*** que les traducteurs utilisent pour ouvrir un fichier source à traduire et interroger la mémoire et les bases de données terminologiques à la recherche de données pertinentes. C'est aussi l'espace de travail dans lequel les traducteurs peuvent écrire leurs propres traductions si aucune correspondance n'est trouvée, et l'interface pour envoyer des paires de phrases terminées à la mémoire de traduction et des paires terminologiques à la base terminologique.

Entente de service : Décrit le type de service que le fournisseur s'engage à fournir. L'entente de service établit le fournisseur, le client, la personne qui peut être contactée en cas de problème, les responsabilités du fournisseur, les responsabilités du client, les exceptions, les changements qui seront notifiés au client, si nécessaire, les détails techniques sur les exigences fonctionnelles (ce que le service est censé faire), l'architecture du service (comment le service est configuré), et les exigences non fonctionnelles (telles que la sécurité, la qualité du service, la facilité d'utilisation, l'enregistrement, etc.).

Entrepôt de données : Système utilisé pour produire des rapports et analyser des données. Les entrepôts de données constituent des dépôts centraux de données intégrées provenant d'une ou de plusieurs sources hétérogènes. Ils comprennent des données actuelles et historiques, et permettent de créer des rapports analytiques destinés aux travailleurs du savoir de l'ensemble de l'entreprise.

Équilibrage de la charge : Dispositif qui agit comme un proxy inversé et distribue le trafic du réseau ou de l'application sur un certain nombre de serveurs. Les équilibreurs de charge sont utilisés pour augmenter la capacité (utilisateurs simultanés) et la fiabilité des applications.

Essai de réception : L'essai d'un système ou d'une unité fonctionnelle effectué par le client sur son site après l'installation et avec la participation de l'entrepreneur pour s'assurer que les exigences contractuelles ont été respectées.

Essais d'acceptation par les utilisateurs (EAU) : Les essais auprès des utilisateurs finaux est la phase où la solution, le système ou l'application est mis à l'essai pour s'assurer qu'il satisfait aux exigences.

Établissement de rapports : Production de rapports normalisés, personnalisés ou ponctuels en fonction des domaines particuliers des renseignements requis qui sont affichés dans le format le plus approprié.

Évaluation de la menace et des risques (EMR) : Processus structuré visant à établir les risques et à fournir des recommandations pour atténuer les risques par l'analyse des ressources essentielles du système ou du service, des cas ou des scénarios de menace potentielle et des vulnérabilités inhérentes.

Évaluation de la sécurité et autorisation (ESA) :

> **Évaluation de sécurité :** Processus continu d'évaluation du rendement des contrôles de sécurité de TI pendant le cycle de vie des systèmes d'information. Ce processus vise à établir la mesure dans laquelle les contrôles sont mis en œuvre adéquatement, fonctionnent comme prévu, et produisent les résultats voulus pour ce qui est de répondre aux besoins opérationnels des ministères en matière de sécurité. L'évaluation de la sécurité soutient l'autorisation en donnant des raisons d'avoir confiance à la sécurité du système d'information.
>
> **Autorisation de sécurité :** Processus continu consistant à obtenir et à maintenir une décision officielle de gestion prise par un cadre supérieur de l'organisation. Ce processus vise à autoriser l'exploitation d'un système d'information et à accepter expressément le risque d'en dépendre pour appuyer un groupe d'activités opérationnelles, en se fondant sur la mise en œuvre d'un ensemble convenu de contrôles de sécurité et sur les résultats de l'évaluation de sécurité continue.

F

Fabricant d'équipement d'origine (FEO) : Terme qui porte un peu à confusion puisqu'il est utilisé pour décrire une entreprise qui a établi une relation spéciale avec des producteurs d'ordinateurs et de TI. Les FEO sont des fabricants qui revendent les produits d'une autre entreprise sous leur propre nom et leur propre marque.

Federal Information Processing Standards (FIPS) (Normes fédérales de traitement de l'information): Ensemble de normes qui décrit les étapes du traitement des documents, les algorithmes de chiffrement et d'autres normes de technologie de l'information que peuvent utiliser les organismes gouvernementaux non militaires et les entrepreneurs et fournisseurs gouvernementaux qui travaillent avec ces organismes.

Federal Risk and Authorization Management Program (FedRAMP): Programme qui offre une approche normalisée d'évaluation de la sécurité, d'autorisation et de surveillance contenue des services d'infonuagerie.

Fiabilité : Mesures qui témoignent de la capacité d'un produit à fonctionner de façon satisfaisante quand il le faut, pour la période requise et dans l'environnement désigné.

Fiches de rendement : Outil de gestion du rendement de la stratégie – rapport semi-structuré, accompagné de méthodes de conception et d'outils d'automatisation pouvant être utilisés pour suivre les activités exécutées et pour surveiller les conséquences découlant de ces actions.

Fichier texte OpenDocument (ODT) : Le fichier texte OpenDocument est un type d'extension de fichier. Ces fichiers sont le plus souvent créés par le programme gratuit de traitement de texte OpenOffice Writer. Les fichiers ODT sont semblables au format populaire de fichier DOCX utilisé pour Microsoft Word.

Format de document portable (PDF) : Il s'agit du format de fichier conçu dans les années 1990 pour présenter des documents, y compris du formatage de texte et des images, peu importe le logiciel, le matériel ou le système d'exploitation.

Formateur : Personne chargée de la formation relative à un service.

Formation des formateurs : Programme de formation conçu pour apprendre aux participants comment offrir aux utilisateurs de la formation en salle de classe et de la formation pratique sur la solution de services.

Forme stockée de caractères (UTF) : Le UTF est un code de caractères qui permet d'encoder tous les caractères possibles, ou points de code, définis dans Unicode. Le plus utilisé, UTF-8, est un code de longueur variable qui utilise des unités de code de 8 bits. Il est conçu pour être compatible vers le bas avec le code ASCII.

Fournisseurs : Entreprise qui peut avoir une ou plusieurs ressources pouvant fournir des services linguistiques au Bureau de la traduction.

G

Gestion de l'identité fédérée : Permet aux applications de partager en toute sécurité les informations d'identité entre plusieurs domaines. Autrement dit, cela signifie que vos utilisateurs n'ont à se connecter qu'à un seul endroit – votre fournisseur d'identité hébergé à l'interne, et toutes vos applications, où qu'elles se trouvent, peuvent faire confiance aux informations que votre fournisseur d'identité certifie au sujet de vos utilisateurs.

Gestion de la charge de travail : Capacité d'attribuer, de prévoir et de gérer les tâches et les calendriers des ressources, y compris la capacité d'affecter des travailleurs à des secteurs de service, de gérer les disponibilités et de répartir également le volume et les types de tâches sur l'ensemble du personnel aussi efficacement que possible et conformément aux objectifs de niveau de service prédéterminés.

Gestion des connaissances : Processus d'officialisation des meilleures pratiques, du matériel de formation et des politiques organisationnelles en vue d'y accéder rapidement et facilement.

Gestion des documents : Coordination et contrôle du flux (stockage, extraction, traitement, impression, acheminement et distribution) de documents électroniques et papier de manière sécuritaire et efficace pour veiller à ce que les personnes autorisées puissent y avoir accès, au besoin.

Gestion des flux de travaux : L'acheminement de l'information vers les ressources en empruntant un chemin de processus prescrit associé à un service particulier qui peut être automatisé et configuré manuellement. Les processus sont configurables en fonction des tâches, des règles opérationnelles, des politiques et de leurs étapes spécifiques (p. ex., analyse, traduction, examen, validation, assurance de la qualité, révision et facturation).

Gestion des incidents : Processus qui consiste à consigner, à enregistrer et à résoudre des incidents. L'objectif de la gestion des incidents est de rétablir le service au client le plus rapidement possible plutôt que de tenter de trouver une solution permanente.

Gestion des justificatifs d'identité : Collecte, suivi (p. ex., documents manquants ou expirés), regroupement et conservation des éléments de preuve (p. ex., attestations, documents juridiques, évaluations de la qualité, attestations de sécurité pour une installation ou une personne, résultats des mises à l'essai des produits, énoncés de l'intégrité des services et documents d'attestation) en ce qui concerne la capacité actuelle et l'expérience d'un fournisseur. Dans la plupart des cas, les justificatifs d'identité des fournisseurs sont fournis par le fournisseur dans une soumission.

Gestion des problèmes : Méthodes et procédures normalisées visant à réduire au minimum les répercussions des problèmes.

Gestion des processus : L'ensemble des activités de planification et de suivi du rendement d'un processus d'affaires. C'est l'application des connaissances, des compétences, des outils, des techniques et des systèmes pour définir, visualiser, mesurer, contrôler, rapporter et améliorer les processus.

Gestion des ressources : Processus d'utilisation des ressources de la façon la plus efficace possible. Il peut s'agit de ressources réelles, comme des biens corporels et de l'équipement, de ressources financières et de ressources en main-d'œuvre, comme des employés.

Gestion des services de technologie de l'information (GSTI) : La gestion des services de TI englobe l'ensemble des activités orientées par les politiques ainsi qu'organisées et structurées en processus et en procédures à l'appui, qui sont réalisées par une organisation en vue de concevoir, de planifier, de fournir, d'exploiter et de contrôler les services de TI offerts aux clients. Ces services comprennent notamment :

a) la gestion du changement – méthodes normalisées pour la gestion efficace des changements opérationnels;
b) la gestion de la configuration – aspects logiques et physiques de l'infrastructure de la TI et autres services de TI;
c) la gestion d'incidents – exploitation au quotidien/contrôles qui aident à rétablir des normes acceptables en matière de pratiques de TI;
d) la gestion des versions – vérification, mise à l'essai et lancement simultanés de changements dans l'environnement de TI;
e) la gestion de problèmes – diagnostic d'incidents pour gérer et éliminer proactivement les erreurs;
f) service de dépannage – gestion d'une plateforme d'interaction centrale pour les opérations et les clients.

Gestion des versions : Méthodes et procédures normalisées visant à intégrer et à faire cheminer la mise en œuvre, l'essai, le déploiement et l'appui du SGDSL.

Gestion du changement : Un processus conçu pour aider à contrôler le cycle de vie des changements stratégiques, tactiques et opérationnels apportés aux services de TI au moyen de procédures normalisées, et dans le but de contrôler le risque et réduire au minimum les perturbations des services de TI et des activités opérationnelles connexes.

Gouvernement du Canada (GC) : L'administration centrale du Canada.

H

Heures converties : Heures d'interprétation converties en fonction du coefficient fourni dans la convention collective des TR (s'applique au personnel à l'interne seulement, par jour, par semaine, par mois, par interprète).

Heures payées pour le temps de déplacement : Nombre d'heures versées à un interprète pour son déplacement (sans calcul de conversion ou de coefficient) par jour, par semaine, par mois, par client, par interprète, par région, par langue, etc.

Hôte : Entité associée à une adresse IP et connectée à un réseau IP.

I

Identification (ID) : La capacité d'identifier de façon unique un utilisateur d'un système ou d'une application ouverte dans le système.

Identification unique (IU) : Permet à un seul justificatif d'authentification – ID utilisateur et mot de passe, carte à puce, jeton de mot de passe unique ou dispositif biométrique – d'accéder à plusieurs systèmes ou à des systèmes différents au sein d'une même organisation. Un système fédéré de gestion des identités fournit un accès unique à de multiples systèmes dans différentes entreprises.

Incident : Tout événement qui ne fait pas partie de l'exploitation normale d'un service et qui cause, ou peut causer, une interruption ou une réduction de la qualité du service.

Indexation : Structure de données qui améliore la vitesse de récupération des données dans un tableau de base de données grâce à des entrées et de l'espace de stockage supplémentaire pour maintenir la structure des données de l'index. Les index sont utilisés pour localiser rapidement les données sans avoir à rechercher chaque ligne d'une table de base de données chaque fois que l'on consulte une table de base de données. Les index peuvent être créés en utilisant une ou plusieurs colonnes d'une table de base de données, fournissant la base à la fois pour des recherches aléatoires rapides et un accès efficace aux enregistrements demandés.

Indicateur de rendement clé : Type de mesure du rendement utilisé pour mesurer la réussite d'une activité particulière.

Information protégée : Renvoie aux dispositions particulières de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* et s'applique aux renseignements personnels, à l'information sur la vie privée et à l'information sur les entreprises de nature délicate. 1) Protégé A (renseignements de nature peu délicate) : s'applique aux renseignements qui, s'ils sont compromis, risqueraient vraisemblablement de porter préjudice à d'autres intérêts que l'intérêt national (p. ex., divulgation de salaires précis). 2) Protégé B (renseignements de nature particulièrement délicate) : s'applique aux renseignements qui, s'ils sont compromis, risqueraient vraisemblablement de causer un préjudice sérieux à des intérêts autres que l'intérêt national (p. ex., perte de réputation ou d'avantage concurrentiel). 3) Protégé C (renseignements de nature extrêmement délicate) : s'applique à un nombre très restreint de renseignements qui, s'ils sont compromis, risqueraient vraisemblablement de causer un préjudice extrêmement sérieux à des intérêts autres que l'intérêt national (p. ex., perte de vie).

Informatique décisionnelle (ID) : Ensemble de techniques et d'outils à utiliser pour la transformation de données brutes en une information valable et utile aux fins de l'analyse des activités opérationnelles.

Infrastructure à clés publiques (ICP) Entrust : Système complet nécessaire à la prestation de services de chiffrement à clés publiques et de signatures numériques dans une grande variété d'applications. Une organisation établit et maintient un environnement de réseautage digne de confiance en gérant les clés et les certificats au moyen d'une infrastructure à clés publiques.

Intégration : Processus qui consiste à regrouper des sous-systèmes dans un seul système et à veiller à ce que ces derniers soient compatibles. Arrangement des systèmes d'information d'une organisation d'une façon qui leur permet de communiquer efficacement ensemble et de regrouper les éléments connexes en un seul système.

Interface : L'interface permet la communication entre logiciels, matériel, dispositifs périphériques, humains ou une combinaison de ceux-ci.

Interface de programmation d'applications (API) : Ensemble de procédures, de protocoles et d'outils pour la création d'applications, y compris les interfaces qui permettent aux composants logiciels et matériels de communiquer entre eux.

Interface utilisateur graphique (IUG) : Permet aux utilisateurs d'interagir avec des appareils électroniques par l'intermédiaire d'icônes graphiques et des indicateurs visuels.

Internet Explorer (IE) : Navigateur Web de Microsoft.

Interopérabilité : Capacité qu'ont les différents systèmes et applications à communiquer, à échanger des données et à utiliser les renseignements qui ont été échangés.

Interprète : Une personne qui interprète ou, plus précisément, qui effectue un transfert linguistique oral de la parole.

J

Jour ouvrable : Tout jour de travail, du lundi au vendredi, à l'exclusion des jours fériés et d'autres congés, et de toute autre journée où le gouvernement du Canada est fermé.

Jours-interprète : Mesure officielle utilisée dans le domaine de l'interprétation à l'échelle internationale.

Un jour-interprète est compté tous les jours où au moins une tâche d'interprétation est attribuée à un interprète (peu importe la durée). Le calcul se fait par jour, par semaine, par mois, par client du BT, par interprète, par région et par langue.

Justificatifs d'identité : Des justificatifs d'identité sont fournis pour authentifier un utilisateur et lui permettre d'avoir accès à des systèmes, à des caractéristiques et à des fonctions en particulier. Il peut s'agir d'une combinaison ID utilisateur et mot de passe, d'un dispositif biométrique, d'un ID utilisateur et mot de passe associés à un mot de passe unique et d'un ID utilisateur et mot de passe associé à des questions personnelles que seul l'utilisateur peut répondre.

K

L

Langage d'interrogation structuré (SQL) : Langage particulier à un domaine utilisé pour la programmation et la conception de la gestion de données stockées dans un système de gestion de base de données relationnelle, ou pour le traitement du flux de données dans le cadre de la gestion du flux de données relationnelle.

Langage de balisage des déclarations de sécurité (SAML 2.0) : Il s'agit d'une norme-cadre qui englobe les profils, les associations et les constructions pour obtenir une identification unique, la fédération et la gestion de l'identité. Le langage de balisage des déclarations de sécurité est un format de données standard ouvert basé sur XML pour l'échange de données d'authentification et d'autorisation entre les parties, en particulier entre un fournisseur d'identité et un fournisseur de services.

Langage hypertexte (HTML) : Le langage standard en création de pages Web et d'applications Web.

Latence (millisecondes) : Cette mesure indique l'intervalle de temps entre la soumission d'un paquet et son arrivée à destination.

Localisation (I10n) : Tâche qui implique la traduction et l'adaptation d'une page Web, d'une application logicielle ou d'un autre produit à une communauté linguistique et culturelle particulière.

Localization Industry Standards Association Quality Assurance (LISA QA) : Organisme suisse de commerce se spécialisant dans la traduction de logiciel en multiples langues naturelles et qui existait de 1990 à février 2011.

Loi sur la protection des renseignements personnels et les documents électroniques **(LPRPDE) :** Cette **loi** canadienne porte sur la protection des données. Elle régit la façon dont les organismes privés recueillent, utilisent et divulguent les **renseignements personnels** dans le cadre de leurs activités commerciales.

M

Matrice de traçabilité des exigences relatives à la sécurité (MTERS) : Grille qui permet de documenter et de voir facilement ce qui est requis relativement à la sécurité d'un système. Les MTERS sont nécessaires dans le cadre de projets techniques pour lesquels il faut tenir compte de la sécurité. En général, les matrices de traçabilité peuvent être utilisées pour tout type de projet, et facilitent la traçabilité entre les exigences et les mises à l'essai. La matrice est une façon de s'assurer qu'il y a une responsabilisation par rapport à tous les processus et il s'agit d'une façon efficace pour l'utilisateur de s'assurer que tout le travail est effectué.

Mémoire de traduction (MT) : Base de données qui stocke des « segments », qui peuvent être des phrases, des paragraphes ou des unités de type phrase qui ont déjà été traduits, afin d'aider les traducteurs humains. Ces segments sont sauvegardés en vue d'être appliqués à des traductions futures.

Mesures : Mesures du rendement qui évaluent les progrès et les tendances au sein d'une organisation.

Métadonnées : Données qui définissent et décrivent d'autres données, et qui servent à identifier, à décrire, à localiser ou à utiliser les systèmes, les ressources et les éléments d'information**.**

Microsoft Office (MS Office) : Suite des applications Microsoft dont Word, Excel, PowerPoint, etc.

Mise à jour du logiciel : Correctifs matériels et/ou logiciels de code qui sont lancés afin de résoudre certains problèmes ou d'activer des fonctionnalités spécifiques.

Mise à niveau du logiciel : Dans les ordinateurs, une mise à niveau est une version plus récente ou un ajout à un matériel ou à un produit logiciel qui est déjà installé ou utilisé.

Modèle de données : Organise des éléments de données (qualitatifs ou quantitatifs) et normalise la façon dont ils interagissent. Il illustre la structure des données de manière détaillée.

N

National Institute of Standards and Technology (NIST): Un laboratoire de métrologie et organisme non réglementaire du département du Commerce des États-Unis. Sa mission est de promouvoir l'innovation et la compétitivité de l'industrie.

Niveau de classification de sécurité : Indicateur du niveau de sensibilité des renseignements du SGDSL précisé par le gouvernement du Canada (classification, abréviation, niveau de sensibilité).

a) Très Secret (TS) TE
b) Secret (S) E
c) Confidentiel (C) E
d) Protégé C (PC) E
e) Protégé B (PB) M
f) Protégé A (PA) F
g) Sans classification (SC) TF
h) Non sensible (NS) TF

Nombre d'entrepreneurs et taux : (taux moyen, taux le plus élevé, taux le plus bas) Les taux sont fixés par jour pour l'interprétation parlementaire et de conférences et par heure pour l'interprétation visuelle. Les taux peuvent exceptionnellement être fixés par activité dans des cas particuliers.

Nombre d'événements par priorité : Les événements sont classés par priorité (A, B ou C) en fonction de divers facteurs (type de réunions, participants, etc.).

Notation des objets du langage Java (JSON) : Format de fichier normalisé ouvert qui utilise un texte interprétable par l'utilisateur pour transmettre des objets de données qui consistent d'attribut – pairs de valeurs et divers types de données.

Notification : Message généré par le système qui avise l'utilisateur qu'une action doit être posée (p. ex., approuver, refuser), ou qu'une action posée nécessite une attention particulière.

Nouvelle version : Version de système, version et préversion d'un logiciel sous licence, peu importe si l'entrepreneur mentionne, ou non, qu'il s'agit d'une « nouvelle version ».

Numéro d'entreprise : Numéro unique qui est donné à une entreprise inscrite par l'Agence du revenu du Canada à titre d'identificateur.

O

Objectif de point de reprise (OPR) : Quantité de données que vous pouvez vous permettre de perdre avant qu'il y ait des répercussions sur les activités commerciales. Par exemple, considérez l'OPR comme le moment où un utilisateur enregistre un document sur lequel il travaille, et si la ***solution du SGDSL*** tombe en panne et que la progression est perdue, quelle part du travail l'utilisateur est-il prêt à perdre avant que cela ne les affecte.

Objectif de temps de reprise (OTR) : Est lié au temps d'arrêt et représente le temps nécessaire à la restauration à partir de l'incident (perturbation) jusqu'au rétablissement des opérations normales pour les utilisateurs. Voici des exemples d'OPR et d'OTR :

> **Niveau 1 :** Applications essentielles à la mission qui nécessitent un OPR et un OTR de moins de 15 minutes.
>
> **Niveau 2 :** Applications essentielles aux activités qui nécessitent un OTR de 2 heures et un OPR de 4 heures.
>
> **Niveau 3 :** Applications non critiques qui nécessitent un OTR de 4 heures et un OPR de 24 heures.

Office Open XML : Aussi appelé de façon non officielle OOXML ou Microsoft Open XML (MOX), Office Open XML est un format de fichier XML compressé développé par Microsoft pour représenter les tableurs, les graphiques, les présentations et les documents de traitement de texte.

Organisation internationale de normalisation (ISO) : L'ISO est un organe de normalisation international composé de représentants de diverses organisations de normalisation nationales.

P

Paramètres configurables : Paramètres prêts à utiliser qui peuvent être modifiés sans qu'il soit nécessaire d'adapter quoi que ce soit, afin de respecter les normes et les exigences du gouvernement du Canada en matière de services, y compris l'architecture de technologie de l'information, la fonctionnalité, le rendement, la disponibilité, la maintenabilité, la sécurité, de même que la continuité des activités et la reprise après sinistre.

Périmètre de sécurité : Limite logique ou physique entourant les ressources et les renseignements accessibles du réseau, contrôlée et protégée contre les accès non autorisés depuis l'extérieur.

Pigiste : Traducteur ou interprète qui facture son travail ou ses services à l'heure, à la journée, à la tâche, etc.

Plan de continuité des services (PCS) : Sous-ensemble du Plan de continuité des activités (PCA) qui englobe la planification de la reprise après sinistre des TI ainsi que la planification plus étendue des TI. Il comprend également les éléments de l'infrastructure et des services de TI.

Plan de reprise après sinistre (PRS) : Un processus documenté ou un ensemble de procédés favorisant la reprise et la protection d'une infrastructure opérationnelle de TI en cas de catastrophe. Un tel plan, habituellement documenté de manière écrite, énonce les procédures précises que doit suivre une organisation en cas de catastrophe. Il s'agit d'un énoncé complet des mesures systématiques devant être prises avant, pendant et après un désastre. Il peut s'agir d'une catastrophe d'origine naturelle, anthropique ou environnementale. Une catastrophe causée par l'homme peut être intentionnelle (p. ex., un acte de terrorisme) ou non intentionnel (p. ex., un accident tel que le bris d'un barrage artificiel).

Plan relatif aux essais d'intégration de la sécurité : Description des étapes à suivre et des essais à effectuer afin de s'assurer que les fonctions de sécurité ont été mises en œuvre de façon adéquate à l'étape de l'intégration de la solution (lorsque les composants de la solution sont assemblés pour former la solution finale).

Plateforme : Composantes polyvalentes de systèmes d'information servant à traiter et à stocker des données électroniques (ordinateurs de bureau, serveurs, dispositifs de réseau et appareils mobiles). Les plateformes sont généralement constituées de matériel serveur, de matériel de stockage, de matériel utilitaire, de logiciels et de systèmes d'exploitation.

Portail : Page Web spécialement conçue pour regrouper de façon uniforme l'information provenant de sources différentes. Habituellement, les renseignements provenant de chaque source d'information sont affichés à un emplacement dédié sur la page; souvent, l'utilisateur peut configurer les sources à afficher. Les variantes des portails comprennent les tableaux de bord des intranets à l'intention des cadres supérieurs et des gestionnaires.

Premier point de contrat (PPC) : Le centre de dépannage ou centre d'appui est le premier palier (point de contact) pour régler les problèmes de base tels que la réinitialisation de mots de passe, l'utilisation de caractéristiques et de fonctions, et le dépannage informatique de base.

Prévention de la perte de données (PPD) : Produits qui, basés sur des politiques centrales, relèvent, surveillent et protègent les données au repos, en mouvement et en cours d'utilisation, grâce à une analyse approfondie du contenu.

Primes de télédiffusion : Conformément à la convention collective des TR :

a) **Interprètes de conférence :** Un supplément de sept dollars (7 $) de l'heure brute d'interprétation est versé au fonctionnaire qui interprète un débat ou une conférence diffusée en direct. Ce supplément étant versé deux (2) fois par exercice financier. À cette fin, le total du temps d'interprétation diffusée en direct est établi au quart (1/4) d'heure le plus rapproché.

b) **Interprètes parlementaires :** Un supplément de cinq dollars cinquante (5,50 $) l'heure brute d'interprétation est versé au fonctionnaire qui interprète les débats de la Chambre des communes. Ce supplément est versé deux (2) fois par exercice financier et, à cette fin, le total du temps d'interprétation est établi quotidiennement au quart (1/4) d'heure le plus rapproché.

Primes multilingues : Conformément à la convention collective des TR :

> Un supplément de soixante dollars (60 $) est ajouté à la rémunération du fonctionnaire qui occupe un poste d'interprète de langues officielles pour chaque jour où il effectue, à la discrétion de l'employeur, de l'interprétation de langues étrangères, peu en importe la nature ou la durée, ce supplément étant versé une fois l'an, après la fin de l'exercice financier.

Processus d'approvisionnement : Processus qui porte sur l'acquisition de biens et de services, de la demande au paiement.

Profil d'utilisateur : Dossier de données propres à l'utilisateur qui définissent son environnement de travail et ses rôles.

Profil de contrôle de sécurité (PCS) : Ensemble de contrôles de sécurité de la TI qu'une organisation établit comme exigences minimales obligatoires pour ses systèmes d'information.

Programme de validation des algorithmes cryptographiques (PVAC) : Le Programme de validation des algorithmes cryptographiques (PVAC) assure la mise à l'essai de validation des algorithmes cryptographiques approuvés par la Federal Information Processing Standards (FIPS) et recommandés par la National Institute of Standards and Technology (NIST) de même que de leurs composantes individuelles. La validation des algorithmes cryptographiques est un prérequis pour la validation des modules cryptographiques.

Programme de validation du module cryptographique (PVMC) : Le Programme de validation du module cryptographique (PVMC) valide les modules cryptographiques en fonction des Federal Information Processing Standards (FIPS) 140-1, *Security Requirements for Cryptographic Modules* (Exigences en matière de sécurité pour les modules cryptographiques) et d'autres normes des FIPS portant sur la cryptographie. La norme FIPS 140-2 (lien externe), Exigences en matière de sécurité pour les modules cryptographiques, a été publiée le 25 mai 2001 et remplace la norme FIPS 140-1.

Project Management Body of Knowledge (PMBOK) : Ce terme fait allusion à l'ensemble des processus, des pratiques exemplaires, de terminologies et des lignes directrices qui sont acceptés à titre de normes dans l'industrie de la gestion de projet.

Projets en environnements contrôlés (PRINCE2) : Il s'agit d'une approche axée sur le processus pour la gestion de projet et il est principalement utilisé dans les paradigmes de TI. PRINCE2 est utilisé pour de nombreux types de projets et peut être appliqué à n'importe quelle étape de la gestion de projet.

Protocole : Ensemble de règles spéciales dont l'objectif est, lorsqu'elles communiquent, l'utilisation d'une connexion de télécommunications. Les protocoles précisent les interactions qui existent entre les entités de communication.

Protocole allégé d'accès annuaire (LDAP) : Protocole d'application ouvert et adapté à tout fournisseur qui est compatible avec la norme de l'industrie et qui permet d'accéder à des services d'annuaires répartis par l'intermédiaire d'un réseau IP et de les maintenir.

Protocole de contrôle de transmission (TCP) : Il s'agit de l'un des principaux protocoles de la suite des protocoles Internet. Il résulte de la mise en œuvre du premier réseau à se servir du protocole Internet (IP). La suite complète est communément appelée TCP/IP. Le protocole de contrôle de transmission (TCP) fournit une

prestation fiable, commandée et sans erreur d'un flux d'octets (bits) entre les applications exécutées sur des hôtes communiquant par l'entremise d'un réseau IP. Les grandes applications Internet, comme le Web, les courriels, l'administration à distance et le transfert des fichiers se fient au TCP.

Protocole de datagramme de l'utilisateur (UDP) : Le protocole de datagramme de l'utilisateur fait partie de la suite des protocoles Internet utilisée par les programmes exécutés sur différents ordinateurs sur un réseau. Le UDP est utilisé pour transmettre de courts messages (datagrammes), mais dans l'ensemble, il s'agit d'un protocole sans connexion et peu fiable.

Protocole de transfert de fichiers (FTP) : Protocole réseau standard servant à transférer des fichiers information entre un client et un serveur sur un réseau informatique.

Protocole de transfert hypertexte sécurisé (HTTPS) : HTTPS, c'est HTTP avec chiffrement SSL ou TLS. SSL (ou TLS) établit un tunnel bidirectionnel sécurisé pour l'envoi de données binaires arbitraires entre deux hôtes. HTTP est un protocole d'envoi de requêtes et de réponses, les requêtes et les réponses étant formées d'en-têtes détaillés et (possiblement) de contenu. HTTP est conçu pour fonctionner au moyen d'un tunnel bidirectionnel pour la transmission de données binaires arbitraires. Lorsque ce tunnel est une connexion SSL/TLS, il s'agit de HTTPS.

Protocole sécurisé de transfert de fichiers (PSTF) : Le Protocole sécurisé de transfert de fichier permet de s'assurer que les données sont transférées de façon sécurisée au moyen d'un flux de données privé et sécuritaire. Il s'agit du protocole de transmission de données standard à utiliser avec le protocole SSH2.

Protocole Transport Layer Security (TLS) : Il s'agit du nouveau nom de SSL. Par précisément, le protocole SSL s'est rendu à la version 3.0; et le TLS 1.0 est « SSL 3.1 ». Les versions du TLS actuellement définies comprennent TLS 1.1 et 1.2. Chaque nouvelle version vient ajouter les fonctions et modifier certains détails internes. Nous disons parfois « SSL/TLS » (voir *HTTPS*).

Q

R

Réaction aux incidents (RI) : Processus par lequel une organisation réagit face à une atteinte à la sécurité ou à une cybermenace, y compris comment l'organisation essaye de gérer les incidences de cette atteinte ou menace. Les plans d'intervention en cas d'incident sont conçus pour mettre à l'essai les capacités de votre entreprise de réagir à un **incident** de sécurité. L'objectif ultime est de gérer la situation de manière à limiter les dommages aux opérations et de réduire le temps de récupération et les coûts.

Really Simple Syndication (RSS) : Type de fil de nouvelles qui permet aux utilisateurs d'avoir accès à des mises à jour du contenu en ligne dans un format normalisé et lisible par un ordinateur. Ces fils de nouvelles peuvent par exemple permettre à un utilisateur de faire le suivi de ce qui est publié sur différents sites Web au moyen d'un seul agrégateur de nouvelles.

Recherche selon la logique floue : Technique d'extraction de texte visant à trouver des résultats correspondants même lorsque les mots-clés sont mal orthographiés ou ne font allusion qu'à un concept.

Répertoire : Espace virtuel permettant de stocker ou de conserver de façon sécuritaire des renseignements pour les réutiliser dans la solution du SGDSL.

Réseau privé virtuel (RPV) : Le RPV est un réseau privé déployé sur un réseau public qui permet aux utilisateurs de transmettre ou de recevoir des données de façon sécurisée sur des réseaux partagés ou publics, comme si leur ordinateur était connecté directement à un réseau privé sécurisé.

Responsable, Agent comptable, Consulté, Informé (RACI) : Un tableau **RACI** est une matrice de l'ensemble des activités ou des pouvoirs décisionnels d'une organisation par rapport à l'ensemble du personnel ou des rôles.

S

Schéma : Structure qui définit l'organisation des données dans une base de données.

Schéma de processus : Schéma qui décrit et présente les processus opérationnels qui sont réalisés par les utilisateurs, les rôles ou les acteurs au sein d'une organisation.

Secrétariat du Conseil du Trésor (SCT) : Le SCT fournit des conseils et des recommandations au comité de ministres du Conseil du Trésor sur la façon dont le gouvernement investit dans les programmes et les services, ainsi que sur la façon dont il en assure la réglementation et la gestion.

Secure Sockets Layer (SSL) : Premières versions du protocole Netscape (AOL).

Segmentation Rules eXchange (SRX) : Il s'agit de la norme adaptée à tous les fournisseurs initialement publiée par LISA (Localization Industry Standards Association) pour décrire comment les outils de traduction et d'autres outils de traitement de la langue segmentent le texte aux fins du traitement.

Segments : Base de données qui stocke des « **segments** » dans une MT, qui peuvent être des phrases, des paragraphes ou des unités de type phrase (en-têtes, titres ou éléments d'une liste) qui ont déjà été **traduits**, afin d'aider les traducteurs humains.

Service d'urgence après les heures (SAH) : Le SAH est responsable de fournir les services linguistiques d'urgence après 17 h la semaine et pendant les fins de semaine et jours fériés.

Service géré par l'entrepreneur : La ***solution du SGDSL*** sera hébergée dans un service géré par l'entrepreneur.

Services publics et Approvisionnement Canada (SPAC) : SPAC est le ministère du gouvernement du Canada responsable des services internes et de l'administration. Il est dirigé par le ministre des Services publics et de l'Approvisionnement.

Services Web : Façon normalisée d'intégrer les applications Web qui utilisent les normes ouvertes XML, SOAP, WSDL et UDDI sur une dorsale de protocole Internet. Les services Web permettent aux organisations de communiquer des données sans avoir de connaissance approfondie des systèmes de technologie de l'information des uns et des autres derrière le pare-feu.

SIGMA (SAP – System Applications and Products) : Gère le soutien en service du système de TPSGC en matière de finances, d'approvisionnement et de biens immobiliers – il s'agit de l'un des systèmes de planification des ressources d'entreprise SAP les plus complets au sein du gouvernement du Canada.

Signature numérique : Transformation cryptographique qui, si elle est ajoutée à un message, à une transaction ou à un dossier, permet au destinataire de vérifier l'identité du signataire et de déterminer si l'information d'origine a été modifiée ou si la signature a été imitée depuis que la transformation a été réalisée.

Single Object Access Protocol (SOAP) : Protocole de messagerie qui permet aux programmes exécutés sur divers systèmes d'exploitation (comme Windows et Linux) de communiquer au moyen du Protocole de transfert hypertexte (HTTP) et de son langage de balisage extensible (XML).

Standardiste automatique : Série de messages enregistrés qui décrivent ce que l'appelant peut faire pour avoir accès aux services particuliers. Un standardiste automatique peut acheminer plusieurs appels simultanés à la personne appropriée.

Stockage : Fonction qui comprend la réception d'un article, sa mise en sécurité et sa récupération, au besoin, pour utilisation, vente ou aliénation.

Structure de répartition des travaux du contrat (SRT) : La structure de répartition des travaux du contrat fait allusion à la partie précise de la structure de répartition qui est associée à un projet précis conçu et maintenu par le vendeur dans le but d'essayer de mettre en œuvre un sous-projet ou une composante du projet pour l'acheteur.

Système d'exploitation (SE) : Programme d'exploitation qui gère les ressources du matériel informatique et les ressources logicielles et qui fournit des services courants pour les programmes informatiques.

Système de gestion des demandes de services linguistiques (SGDSL) : Type de logiciel permettant d'automatiser de nombreuses parties du processus de traduction des langues humaines et de maximiser l'efficacité du traducteur, notamment :

> Outil de traduction – L'interface de traduction que les traducteurs, les réviseurs et autres utilisent pour créer les traductions.
>
> Outil de gestion terminologique – Un outil qui permet de créer, sauvegarder et gérer des bases de données de termes spécifiques pertinents pour l'entreprise.

Système de gestion du contenu (SGC) : Application informatique qui permet la création et la modification de contenu numérique. Il prend généralement en charge plusieurs utilisateurs dans un environnement collaboratif. La plupart des SGC comprennent des fonctions de publication sur le Web, de gestion des formats, d'édition de l'historique et de contrôle des versions, d'indexation, de recherche et d'extraction.

Système de production : Ensemble des systèmes informatiques en temps réel et des systèmes informatiques axés sur les données réelles exécutés dans l'environnement de production utilisé au sein du gouvernement du Canada, qui interagira et communiquera avec des programmes, qui exécutera des programmes ou qui transférera des données dans le système de gestion de traduction afin de traiter les tâches quotidiennes du gouvernement du Canada en matière d'approvisionnement, et de réaliser les activités liées à l'exécution d'un ou de plusieurs systèmes d'une manière bien visible, de façon qu'elles soient accessibles et appuyées par les utilisateurs finaux de ces systèmes.

T

Tableau de bord : Interface facile à lire, en temps quasi réel, qui affiche l'état actuel (aperçu) de renseignements précis.

Tableur Microsoft Excel (XLS, XLSX) : Applications Microsoft utilisées pour le stockage, l'organisation et la manipulation de données.

Taxonomie : Façon de classifier et de structurer l'information.

Technologie de l'information (TI) : Utilisation d'ordinateurs pour entreposer, extraire, transmettre et manipuler des données ou de l'information, souvent dans le contexte commercial ou d'autres activités. La TI est considérée comme un sous-ensemble de la technologie de l'information et des communications.

Tel écran – Tel écrit (What You See Is What You Get : WYSIWYG) : Éditeur ou programme qui permet au développeur de **voir** à quoi ressemblera le résultat final pendant la création de l'interface ou du document.

Temps réel : Données actives qui sont utilisées dans ***La solution SGDSL*** à un moment donné.

Temps utilisable réel : Temps réel pendant lequel un service est opérationnel sans interruption.

Téraoctet (To) : Mesure de la capacité de stockage informatique correspondant à mille milliards d'octets et plus précisément à 1 024 gigaoctets (Go).

TermBase eXchange (TBX) : Norme internationale pour la représentation et l'échange d'informations terminologiques.

Traçabilité : Capacité à vérifier l'historique, l'emplacement ou l'utilisation d'un article au moyen d'identifications enregistrées et consignées.

Traduction assistée par ordinateur (TAO) : Forme de traduction par laquelle un traducteur humain utilise du matériel informatique pour appuyer et faciliter le processus de traduction.

Traduction automatique : Outil qui traduit automatiquement le contenu sans intervention humaine.

Traitement analytique en ligne (TAEL) : Est caractérisé par le volume relativement faible de transactions. Les requêtes sont souvent très complexes et impliquent des regroupements. Pour les systèmes de TAEL, le temps de réponse sert à mesurer l'efficacité. Les applications de TAEL sont beaucoup utilisées aux fins des techniques d'exploration de données. Dans les bases de données de TAEL, on y trouve des données historiques et regroupées, stockées dans des schémas multidimensionnels (habituellement un schéma en étoile).

Traitement de transactions en ligne (TTL) : Est caractérisé par le nombre élevé de transactions rapides effectuées en ligne (INSÉRER, METTRE à JOUR, SUPPRIMER). L'objectif principal des systèmes de TTL est d'assurer le traitement très rapide des requêtes, de maintenir l'intégrité des données dans des environnements à accès multiples et de mesurer l'efficacité selon le nombre de transactions par seconde. Dans la base de données de TTL, les données qui s'y trouvent sont complètes et actuelles et le schéma utilisé pour sauvegarder les bases de données transactionnelles est le modèle d'entité (habituellement la 3NF).

Transfert : Passage d'un ancien système (matériel ou logiciel) vers un nouveau. Il s'agit du moment où le nouveau système devient opérationnel.

Transfert d'état représentationnel (REST) : Style architectural qui définit un ensemble de contraintes et de propriétés qui reposent sur HTTP.

Translation Memory Exchange (TMX 1.4B) : Fichier créé dans le format Translation Memory Exchange (TMX), une norme XML ouverte utilisée pour échanger des données de mémoire de traduction (MT) créées par la traduction assistée par ordinateur (TAO) et des applications de localisation; peut enregistrer des mots ou des phrases qui ont été traduits d'une langue à une autre et pour transférer la mémoire de traduction entre différents outils et fournisseurs.

U

Unité centrale de traitement (UCT) : S'entend des circuits électroniques d'un ordinateur qui exécutent les instructions fournies par un programme en moyen de calculs arithmétiques de base et d'opérations logiques, de contrôles et d'entrées-sorties précisés dans les instructions.

Utilisateur : Toute personne qui possède un compte lui permettant d'utiliser la solution du **SGDSL**.

V

Valeurs séparées par des virgules (CSV) : Un format de fichier simple utilisé pour stocker des données tabulaires comme des feuilles de calculs ou des bases de données. Les fichiers en format CSV peuvent être importés et exportés de programmes qui stockent les données dans des tableaux, comme Microsoft Excel.

Vérification et responsabilité (AU) : Contrôles de sécurité qui permettent de recueillir, d'analyser et de stocker des rapports de vérification liés aux interventions de l'utilisateur dans le système d'information.

Vérification : Un examen des contrôles de gestion en place au sein d'une infrastructure de technologie de l'information (TI). L'évaluation des preuves obtenues permet de déterminer si les systèmes d'information protègent les biens, maintiennent l'intégrité des données et fonctionnent efficacement pour permettre à l'organisation d'atteindre ses objectifs.

Version du logiciel : Version qui a généralement franchi différentes étapes de son développement, comme alpha, beta, susceptible d'être diffusé, disponibilité générale, version de production.

Virtualisation : Logiciel qui sépare les infrastructures physiques pour créer diverses ressources dédiées. Le logiciel de virtualisation permet d'exécuter plusieurs systèmes d'exploitation et de multiples applications sur le même serveur en même temps. La technologie sur laquelle repose la virtualisation est connue sous le nom de moniteur de machines virtuelles ou gestionnaire virtuel, qui sépare les environnements de calcul de l'infrastructure physique réelle. Cela est possible en installant un hyperviseur en plus de la couche matérielle, où la **solution du SGDSL** est ensuite installée. Un hyperviseur ou un moniteur de machines virtuelles est un logiciel, un micrologiciel ou du matériel qui crée et exécute des machines virtuelles. Un ordinateur sur lequel un hyperviseur exécute une ou plusieurs machines virtuelles est appelé machine hôte, et chaque machine virtuelle est appelée machine invitée.

Visualisation de données : Méthode qui consiste à placer les données dans un contexte visuel ou graphique afin de communiquer clairement et efficacement des renseignements aux utilisateurs (p. ex., une carte est une méthode qui permet de visualiser les régions du pays qui reçoivent le plus de précipitations).

Voies de communication des demandes de soutien (VCDS) : Voies de communication que peuvent offrir les entreprises aux clients pour obtenir du soutien.

W

X

XLIFF (XML Localisation Interchange File Format) : Il s'agit d'un format XML utilisé pour normaliser la transmission des données vers et depuis les outils à chaque étape du processus de localisation. Il normalise les éléments suivants :

Traitement de contenu localisé
Exploitation de mémoires de traduction et de glossaires
Interaction avec les systèmes de gestion de la traduction, la traduction automatique et les

outils de TAO
Gestion des flux de travaux de localisation

XLIFF est un format XML créé pour normaliser la façon dont les données localisables sont transmises entre les différentes étapes du processus de localisation, tout en assurant l'interopérabilité entre les divers outils utilisés. Les fichiers XLIFF sont des documents bilingues contenant le contenu à localiser, les traductions correspondantes, ainsi que toutes les données auxiliaires qui rendent le processus de localisation efficace ou même possible. Les données de la langue source et de la langue cible dans les fichiers XLIFF sont constamment synchronisées pendant le processus.

En tant que norme ouverte, XLIFF vise à éliminer le besoin de formats exclusifs. Il permet également l'interopérabilité, l'automatisation des flux de travaux et l'intégration des règles à la source. XLIFF normalise des aspects comme le traitement du contenu localisé, l'exploitation des mémoires de traduction et des glossaires, l'interaction avec les outils de TAO, les systèmes de gestion de la traduction et la traduction automatique, ainsi que la gestion de l'ensemble des flux de travaux de localisation.

Y

Z

9 APPENDICE B – ACRONYMES

Acronyme	Description
Architecte de la GI	Architecte de la gestion de l'information
ANS	Accord sur les niveaux de service
ARV	Analytique, rapports et vérification
API	Interface de programmation d'applications
AQ	Assurance de la qualité
ARO	Analyse des répercussions sur les opérations
AT	Autorisations de tâches
BT	Bureau de la traduction
CASCO	Comité pour l'évaluation de la conformité
CCC	Comité consultatif sur le changement
CDEQ de TAUS	Cadre dynamique d'évaluation de la qualité de TAUS
CDSS	Conception détaillée des services de sécurité
CEF	Common Event Format
CEI	Commission électrotechnique internationale
CGSS	Conception générale des services de sécurité
COS	Centre des opérations de sécurité
COTS	Commercial sur étagère
CPVP	Commissariat à la protection de la vie privée du Canada
CST	Centre de la sécurité des télécommunications
CSV	Valeurs séparées par des virgules
DGDPI	Direction générale du dirigeant principal de l'information
DOC	Document, ou fichier texte ASCII avec des codes de formatage de texte dans le texte; utilisé par de nombreux logiciels de traitement de texte
DP	Demande de propositions
DSIC	Direction de la sécurité industrielle canadienne
EAU	Essais d'acceptation par l'utilisateur
ED	Entrepôt de données
EDT	Énoncé des travaux
ESA	Évaluation de sécurité et autorisation
ETC	Extraction, transfert et chargement
FedRAMP	Federal Risk and Authorization Management Program
FEO	Fabricant d'équipement d'origine
FIPS	Federal Information Processing Standards
FTP	Protocole de transfert de fichiers
GC	Gouvernement du Canada
GSTI	Gestion des services des technologies de l'information

Acronyme	Description
HTML	Langage de balisage hypertexte
HTTPS	Protocole de transfert hypertexte sécurisé
ICP Entrust	Infrastructure à clés publiques Entrust
ID	Identification
IE	Internet Explorer
II	Intervention en cas d'incident
IRC	Indicateur de rendement clé
ISO	Organisation internationale de normalisation
ITIL	Information Technology Infrastructure Library (bibliothèque de l'infrastructure des technologies de l'information)
IU	Identification unique
IUG	Interface utilisateur graphique
JSON	Notation des objets du langage Java
LDAP	Protocole allégé d'accès annuaire
LISA QA	Assurance de la qualité – Localization Industry Standards Association
LPRPDE	Loi sur la protection des renseignements personnels et les documents électroniques
LVERS	Liste de vérification des exigences relatives à la sécurité
MI	Messagerie instantanée
MPSSU	Modes de prestation de services de soutien aux utilisateurs
MS Office	Microsoft Office
MT	Mémoire de traduction
MTERS	Matrice de traçabilité des exigences relatives à la sécurité
NIST	National Institute of Standards and Technology
OCCI	Open Cloud Computing Interface
ODT	Format texte OpenDocument
OPR	Objectif de point de reprise
OSS	Organisme de service spécial
OTR	Objectif de temps de reprise
PCS	Profil de contrôle de sécurité
PCS	Plan de continuité des services
PDF	Format de document portable
PI	Propriété intellectuelle
PMBOK	Project Management Body of Knowledge
PPC	Premier point de contact
PRINCE2	Projets en environnements contrôlés
PVAC	Programme de validation des algorithmes cryptographiques
PVMC	Programme de validation des modules cryptographiques
RA	Renseignements d'affaires

Acronyme	Description
RACI	Responsable, agent comptable, consulté et informé
REST	Transfert d'état représentationnel
ROC	Reconnaissance optique de caractères
RPV	Réseau privé virtuel
RS	Reprise après sinistre
SA	Standardiste automatique
SAH	Service d'urgence après les heures
SAML 2.0	Langage de balisage des déclarations de sécurité SAML 2.0
SAP	System Applications and Products
SCT	Secrétariat du Conseil du Trésor
SE	Système d'exploitation
SGC	Système de gestion du contenu
SGDSL	Système de gestion des demandes de services linguistiques
SOAP	Protocole simple d'accès aux objets
SPAC	Services publics et Approvisionnement Canada
SPC	Services partagés Canada
SQL	Langage d'interrogation structuré
SRTC	Structure de répartition du travail contractuel
SRX	Segmentation Rules eXchange
SSH	Secure Shell
SSL	Protocole sécurisé de cryptage
SW	Services Web
TA	Traduction automatique
TAEL	Traitement analytique en ligne
TAO	Traduction assistée par ordinateur
TBX	TermBase Exchange
TCP	Protocole de contrôle de transmission
TI	Technologies de l'information
TLS	Sécurité de la couche transport
TMX	Translation Memory Exchange
To	Téraoctet
TTL	Traitement de transactions en ligne
UCT	Unité centrale de traitement
UTF	Forme stockée de caractères
VR	Vérification et responsabilité
WCAG	Directives pour l'accessibilité aux contenus Web
WPD	Document WordPerfect
WYSIWYG	Tel écran - tel écrit
XLIFF	Format d'échange de fichier de localisation XML

Acronyme	Description
XLS	Tableur Microsoft Excel
XLSX	Classeur Office Open XML (tableurs)
XML	Langage de balisage extensible

10 APPENDICE C – RAPPORTS DU BUREAU DE LA TRADUCTION

Le tableau suivant présente les catégories et les types de rapports.

Catégorie de rapport	Type de rapport
1.0 Rapports sur la production	a) Nombre de mots, de projets au cours d'une période b) Répartition des projets par client, demandeur, spécialité ou domaine, type de tâche, type de document c) Affectation des tâches à l'interne et à l'externe d) Livraison à temps et en retard e) Demandes urgentes f) Service d'urgence après les heures (SAH) g) Demandes de changement d'échéance h) Sommaire selon le type de travail et la spécialisation
2.0 Rapports sur la productivité	a) Feuilles de temps par ressource(s) b) Productivité des ressources c) Détails des tâches effectuées par ressource(s) d) Détails des tâches et du temps consacrés à un projet e) Détails des tâches et du temps consacrés à un projet par ressource(s) f) Heures supplémentaires par direction, par division et par ressource(s) g) Volume (heures et mots) par spécialité, par direction, par division et par ressource(s) h) Nombre de dossiers d'incident traités par ressource(s) i) Nombre de transactions par ressource(s)
3.0 Rapports financiers	a) Revenus par client, domaine, ressource(s), projet, type de tâche b) Coûts internes et externes par client c) Coûts par ressource(s) interne(s) et externe(s) d) Coûts par centres de coûts e) Coûts par types de tâches f) Coûts détaillés par clients g) Comptes débiteurs et comptes créditeurs
4.0 Rapports à la haute direction	a) Rapports sommaires b) Répartition des projets par clients et demandeurs c) Analyse coûts-avantages d) Livraison à temps et en retard e) Demandes urgentes f) Service d'urgence après les heures (SAH) g) Demandes de changement d'échéance h) Coûts par centres de coûts i) Coûts détaillés par clients j) Comptes débiteurs et comptes créditeurs
5.0 Rapports sur les outils	a) Nombre de mots obtenus et économies de coûts par type de mémoire utilisé b) Statistiques globales sur la redondance par période c) Pourcentage de segments traduits à l'aide d'outils de TAO utilisés tels quels dans les traductions finales

Catégorie de rapport	Type de rapport
6.0 Rapports sur l'interprétation	Volume Services d'interprétation de conférences et d'interprétation parlementaire : a) Jours-interprète b) Heures converties c) Répartition de la charge de travail à l'interne et à l'externe Services d'interprétation de conférences, d'interprétation parlementaire et d'interprétation visuelle : d) Nombre d'heures de travail par jour, semaine, mois, client, interprète, région et langue e) Nombre d'heures de déplacement rémunérées par jour, semaine, mois, client, interprète, région et langue f) Nombre de contrats (ouverts et ponctuels) par jour, semaine, mois, client, interprète, région et langue g) Nombre d'activités par jour, semaine, mois, client, interprète, région et langue Normes de service Services d'interprétation de conférences, d'interprétation parlementaire et d'interprétation visuelle : a) Nombre d'activités refusées b) Temps requis pour traiter une demande d'interprétation c) Temps requis pour facturer une demande d) Temps requis pour affecter des interprètes à une activité Autres Services d'interprétation de conférences et d'interprétation parlementaire : a) Nombre d'entrepreneurs et taux horaires et quotidiens (taux moyen, taux le plus élevé, taux le moins élevé) b) Cote de sécurité : rapport sur l'interprète c) Primes de télédiffusion d) Nombre d'activités modifiées après avoir obtenu la confirmation du client (contrat signé) e) Nombre d'activités rétablies après une annulation f) Primes au multilinguisme g) Aide offerte, aide reçue h) Affectations en région éloignée ou hybrides i) Nombre d'activités par priorité (interprétation de conférences)

11 APPENDICE D – RESPONSABILITÉ DES RESSOURCES EN SERVICES PROFESSIONNELS

Gestionnaire de projet
Les responsabilités pourraient comprendre ce qui suit, sans toutefois s'y limiter : • effectuer la planification générale des projets en fonction de mandats, d'estimations, de l'étendue de tâches et de calendriers préétablis; • gérer, surveiller et prévoir l'exécution des projets; • prendre des mesures correctives au besoin pour exécuter les projets conformément à l'étendue des tâches, aux exigences de qualité, aux échéances et au budget (y compris la gestion des modifications de l'étendue des tâches et l'atténuation des risques); • assurer la gestion des intervenants internes et externes grâce à des communications efficaces; • gérer du début à la fin des projets tactiques dont l'envergure varie; • tenir à jour les plans existants, les outils du BGP, les procédures et les systèmes utilisés au sein du BGP qui sont nécessaires pour gérer et orienter les activités d'élaboration du BGP; • élaborer et produire des procédures et des plans nouveaux (par écrit et assujettis à l'approbation du ou des responsables du projet) demandés par la direction pour gérer et orienter les activités d'élaboration du BGP; • planifier, organiser et coordonner toutes les activités associées à un projet attribué, y compris tous les aspects concernant les finances, la planification et l'ordonnancement; • définir et documenter les objectifs du projet et déterminer les exigences budgétaires; • produire et tenir à jour des structures de répartition du travail et des calendriers intégrés; • analyser les calendriers intégrés pour cerner les priorités, les activités et les incompatibilités, et proposer des solutions aux gestionnaires de projet de niveau supérieur et autres; • communiquer les plans, les développements et l'avancement des travaux aux gestionnaires du client; • gérer la mise en œuvre des processus de gestion suivants au niveau de la Direction pour ce qui est des problèmes, des risques, de la qualité, du rendement et du changement; • gérer des équipes de projet conformément au mandat du projet (y compris les attributions de tâches et les examens du rendement); • planifier et coordonner les activités du personnel du projet et d'autres fournisseurs de soutien; • gérer les membres de l'équipe dans les limites du projet; • négocier les modifications concernant la portée du projet, les ressources et le calendrier avec les intervenants; • contribuer aux améliorations du cycle de vie des projets grâce aux leçons retenues et aux archives de projet; • rendre compte à un gestionnaire organisationnel de niveau intermédiaire ayant autorité sur la plupart des membres de l'équipe du projet; • gérer des projets pouvant être sous la conduite d'un gestionnaire de projet d'un niveau plus élevé, subordonné à d'autres coordonnateurs et chefs de projet ainsi qu'à d'autres gestionnaires de projet de niveau supérieur et de la direction.
Analyste des systèmes
Les responsabilités pourraient comprendre ce qui suit, sans toutefois s'y limiter : • élaborer la documentation relative aux exigences, à la faisabilité, aux coûts, à la conception et aux spécifications des systèmes;

- mettre en œuvre les systèmes en vue d'appuyer des projets, des ministères, des organisations ou des entreprises;
- répondre aux exigences opérationnelles par des spécifications et une conception de systèmes adéquate;
- analyser et recommander des options et d'autres solutions possibles;
- élaborer des spécifications techniques pour l'élaboration, la conception et la mise en œuvre de systèmes.

Spécialiste de la conversion de données

Les responsabilités pourraient comprendre ce qui suit, sans toutefois s'y limiter :

- superviser toutes les installations pour le processus de conversion;
- établir les correspondances et les interfaces, simuler les opérations de conversion, apporter les améliorations requises, effectuer la conversion et vérifier l'exactitude et l'intégralité des données converties;
- établir des rapports professionnels et étroits avec tous les clients, interagir efficacement avec les membres du personnel client de tous les niveaux et fournir du soutien en matière de conversion;
- analyser et coordonner les conversions de fichiers de données;
- importer des fichiers en provenance de plateformes hétérogènes.

Analyste d'affaires

Les responsabilités pourraient comprendre ce qui suit, sans toutefois s'y limiter :

- créer et documenter les énoncés concernant les solutions de rechange prises en considération;
- effectuer des analyses des exigences fonctionnelles afin de déterminer les flux d'information et de procédures et les flux décisionnels;
- évaluer les procédures et les méthodes existantes, et définir et décrire des éléments comme le contenu de la base de données, la structure et les sous-systèmes d'application;
- définir et décrire les interfaces des opérations manuelles vers les opérations automatisées au sein des sous-systèmes d'application, vers les systèmes externes, et entre les nouveaux systèmes et les systèmes existants;
- établir les critères d'essais d'acceptation avec le client;
- appuyer et employer les méthodologies ministérielles sélectionnées.

Expert-conseil en restructuration des processus opérationnels

Les responsabilités pourraient comprendre ce qui suit, sans toutefois s'y limiter :

- examiner les processus de travail et la structure organisationnelle existants;
- analyser les exigences fonctionnelles afin de déterminer les flux d'information et de procédures et les flux décisionnels;
- cerner les processus susceptibles d'être conçus à nouveau; créer le prototype des solutions possibles, fournir de l'information sur les compromis et recommander une option à suivre; déterminer les modifications à apporter aux processus automatisés;
- donner des conseils spécialisés concernant la définition de nouvelles exigences et possibilités pour l'application de solutions efficaces et efficientes; déterminer et communiquer les coûts préliminaires des options;

- donner des conseils spécialisés quant à l'élaboration et l'intégration de modèles de processus et d'information entre les processus opérationnels afin d'éliminer les redondances de processus et d'information;
- déterminer et recommander de nouveaux processus et de nouvelles structures organisationnelles;
- offrir des conseils spécialisés sur de nouveaux processus et changements organisationnels et/ou contribuer à leur mise en œuvre;
- documenter le flux de travaux;
- utiliser des outils logiciels de modélisation des opérations, des flux des travaux et de l'organisation.

12 APPENDICE E – CALCUL DE LA CHARGE DE TRAVAIL D'INTERPRÉTATION ET EXEMPLE

Le texte qui suit est un extrait de la convention collective des traducteurs. Il fait état de l'information utilisée pour calculer le nombre total d'heures travaillées par les employés interprètes des services d'interprétation de conférences et d'interprétation parlementaire.

12.1 HEURES DE TRAVAIL – INTERPRÈTES

a) La journée normale de l'interprète comporte en moyenne six (6) heures d'interprétation si ce dernier fait partie d'une équipe de trois (3) interprètes dans une réunion à deux langues de travail, dans les deux sens avec une seule cabine (ou d'une équipe de deux (2) interprètes travaillant dans un seul sens dans une réunion à au moins trois (3) langues de travail) ou environ quatre (4) heures d'interprétation s'il fait partie d'une équipe de deux (2) interprètes dans une réunion à deux langues de travail, dans les deux sens avec une seule cabine.

b) L'effectif et la composition des équipes d'interprètes sont déterminés en fonction de la charge de travail.

I. Effectif minimal en interprétation simultanée :
Pour les réunions à deux langues de travail, dans les deux sens avec une seule cabine : trois (3) interprètes pour jusqu'à six (6) heures, (étant entendu qu'une équipe ne devrait normalement pas travailler plus de quatre (4) heures consécutives);

Deux (2) interprètes pour jusqu'à quatre (4) heures (étant entendu qu'une équipe ne devrait normalement pas travailler plus de trois (3) heures consécutives). Pour les réunions à trois (3) langues de travail : au moins deux (2) interprètes par cabine travaillant dans un seul sens pour jusqu'à six (6) heures (étant entendu qu'une équipe ne devrait normalement pas travailler plus de quatre (4) heures consécutives).

Pour les réunions à quatre (4) langues de travail ou plus : au moins deux (2) interprètes par cabine travaillant dans un seul sens pour jusqu'à six (6) heures, et trois (3) interprètes lorsque les conditions le justifient (étant entendu qu'une équipe ne devrait normalement pas travailler plus de quatre (4) heures consécutives).

À la Chambre des communes, les équipes sont constituées de trois (3) interprètes par cabine et ne devraient normalement pas travailler plus de six (6) heures consécutives. L'employeur, après consultation avec l'Association, organise le roulement des interprètes en conséquence.

II. En interprétation consécutive, chuchotée et d'accompagnement, l'effectif est normalement d'au moins deux (2) interprètes pour une journée de six (6) heures.

c) Le total des heures de travail peut varier selon les besoins opérationnels. Cependant, les heures de travail sont équilibrées mensuellement ou si possible deux fois par mois, l'employeur faisant tout effort raisonnable pour ne pas imposer plus de trente-sept virgule cinq (37,5) heures par semaine, en général. À cette fin, la durée de travail est mesurée en heures, l'heure d'interprétation valant une virgule deux cinq (1,25) heure de travail s'il s'agit d'une équipe de trois (3) interprètes et une virgule huit sept cinq (1,875) heure de travail s'il s'agit d'une équipe de deux (2) interprètes dans une réunion à deux (2) langues de travail, dans les deux sens avec une seule cabine.

En interprétation chuchotée, consécutive ou d'accompagnement, l'heure d'interprétation vaut une virgule huit sept cinq (1,875) heure de travail quand l'interprète est affecté seul et une virgule deux cinq (1,25) heure de travail quand il fait partie d'une équipe.
Dans le calcul des heures de travail, sont pris en compte toutes les fonctions expressément autorisées par l'employeur, les congés et les jours fériés.

d) En général, les affectations se font à l'intérieur d'une plage qui commence à l'heure pour laquelle l'interprète est convoqué et qui se termine douze (12) heures plus tard. Le temps d'interprétation de chaque affectation est compté en minutes à partir de l'heure inscrite au programme de l'interprète jusqu'au moment où sa prestation prend fin.

e) Sous réserve des besoins opérationnels, l'employeur prévoit normalement, en établissant le programme de l'interprète, douze (12) heures de battement entre la fin de la journée de travail de l'interprète et le début de sa plage suivante.

f) Sous réserve des besoins opérationnels, l'employeur accorde à l'interprète deux (2) jours de repos consécutifs au cours d'une période de sept (7) jours civils. S'il est impossible de les accorder, ces jours de repos sont remis le plus tôt possible par le jeu de l'équilibrage prescrit à l'alinéa c).

g) Conformément à l'alinéa c), l'employeur affiche les heures de travail hebdomadaires et cumulatives des interprètes; au service des Conférences, il affiche en outre, toutes les deux (2) semaines, le programme des affectations des deux (2) semaines qui suivent.

h) L'interprète dont l'affectation en interprétation est annulée et qui n'est pas réaffecté pour une période équivalente au cours de la même plage, est réputé avoir effectué des fonctions autres que de l'interprétation pendant la partie non travaillée de l'affectation prévue.

i) L'interprète dont l'employeur exige qu'il soit disponible pendant une période précise doit pouvoir être joint à un numéro de téléphone connu et doit être en mesure de rentrer au travail le plus rapidement possible en cas de rappel. Cette période fait partie de la plage aux fins de l'alinéa d).

Remarque : Les coefficients permettent de convertir les heures de façon à établir le volume de travail par jour, par semaine et par mois. Les jours de repos sont aussi accordés en fonction du nombre d'heures de travail par semaine ou par mois. Les coefficients sont utilisés au quotidien pour calculer et répartir la charge de travail, et une ou deux fois par mois pour équilibrer les heures, par exemple pour prévoir les jours de repos.

12.2 EXEMPLE DE CALCUL – HEURES DE TRAVAIL – INTERPRÈTES

Jour	Activité	Calcul	Total (heures)
Lundi	4 h d'interprétation (2 interprètes par cabine travaillant dans les deux sens)	4 * 1,875	7,5
Mardi	Jour de repos		7,5
Mercredi	8 h d'interprétation (3 interprètes par cabine travaillant dans les deux sens)	8 * 1,25	10
Jeudi	4 h de traduction 2 h d'interprétation (3 interprètes par cabine travaillant dans les deux sens)	4 + (2*1,25)	6,5
Vendredi	8 h d'interprétation (3 interprètes par cabine travaillant dans les deux sens)	8 * 1,25	10
Samedi	N'a pas travaillé		
Dimanche	2 h d'interprétation (2 interprètes par cabine travaillant dans les deux sens)	2 * 1,875	3,75
		Total de la semaine	45,25 h

13 APPENDICE F – LANGUES ET FORMATS DE FICHIERS DU BUREAU DE LA TRADUCTION

13.1 LANGUES

Langues prises en charge par le Bureau de la traduction	
Afrikaans	Javanais
Albanais	Kannada
Algonquin	Kaska
Allemand	Kazakh
Amharique	Kinyarwanda
Anglais	Kirghiz
Arabe	Kirundi
Arménien	Kurde
Assamais	Kwak'wala
Assyrien	Lao
Atikamekw	Latin
Awadhi	Letton
Azerbaïdjanais	Lil'wat
Azéri	Lingala
Bambara	Lituanien
Basque	Luganda
Bengali	Luyia
Biélorusse	Macédonien
Bihari	Malais
Bilen	Malayalam
Birman	Malécite
Bislama	Malgache
Blackfoot	Maltais
Boharme	Mandarin - chinois (interprétation)
Bosniaque	Mandingue
Brésilien	Marathi
Bulgare	Michif
Buriat	Micmac
Cambodgien	Micmac (Pacifique)
Cantonais - Yue (interprétation)	Micmac (Smith-Francis)
Carrier	Mina
Catalan	Mohawk
Cebuano	Mongol
Chilcotin	Montagnais
Chinois	Mowachaht
Chinois (simplifié)	Naskapi
Chinois (traditionnel)	Néerlandais
Coréen	Népalais
Créole	Nisga'a
Cri	Norvégien
Cri de Moose	Nunavik

Langues prises en charge par le Bureau de la traduction	
Cri des bois	Nuu Chah Nulth
Cri des marais	Ojibwé
Cri des marais – Centre	Ojibwé de Rainy River
Cri des marais – Manitoba – caractères romains	Oji-cri
Cri des marais – Manitoba – écriture syllabique	Oowekyala
Cri des marais – Ontario	Oromo
Cri des marais – Saskatchewan	Oudi
Cri des plaines	Ouïgour
Cri du Nord du Québec	Ourdou
Cri du Québec	Ouzbek
Croate	Pachto
Dakota	Pendjabi
Danois	Pendjabi (écriture arabe)
Dari	Persan
Dénésuline	Polonais
Ditidaht	Portugais
Dogrib	Pular
Duri	Roumain
Edo	Russe
Esclave du Nord	Salish de la côte
Esclave du Sud	Sanskrit
Espagnol	Saulteaux
Espéranto	Secwepemctsin
Estonien	Serbe
Éwé	Serbo-croate
Fanti	Setswana
Féroïen	S'gaw Karen
Filipino	Shona
Finnois	Sindhi
Flamand	Singhalais
Français	Slovaque
Fulfulde	Slovène
Gaélique écossais	Somali
Gallois	Soussou
Géorgien	Stoney
Goudjarati	Suédois
Grec	Swahili
Grec ancien	Tadjik
Gwich'in	Tagalog
Halq'eméylem	Tamil
Hébreu	Tatar
Hébreu rabbinique	Tchèque
Hindi	Tchétchène
Hongrois	Telugu
Hul'q'umi'num	Thaï
Igbo	Tibétain
	Tigrigna

Langues prises en charge par le Bureau de la traduction	
Ilocano	Toro
Ilongo	Tshiluba
Inconnue	Turc
Indonésien	Tutchone du Nord
Innu-aimun	Twi
Inuinnaqtun	Ukrainien
Inuktitut	Vietnamien
Inuktitut du Labrador	Vieux portugais
Inuvialuktun	Wolof
Irlandais	Yiddish
Islandais	Yorouba
Italien	Zoulou
Japonais	

13.2 FORMATS DE FICHIERS

Format de fichier (extension)	Description du format de fichier
xls, xlsx, xlsb	Document Excel
xltx, xltm, xlt	Modèle Excel
csv, prn, dif, slk	Fichier de valeurs pouvant être ouvert dans Excel
xla, xlam	Fichier de macro Excel
ods	Équivalent d'Excel dans OpenOffice
doc, docx, docm	Document Word
dot, dotx, dotm	Modèle Word
odt	Équivalent de Word dans OpenOffice
wpd	Document WordPerfect
lwp	Document WordPro
ppt, pptx, pptm	Document PowerPoint
potx, potm, pot	Modèle PowerPoint
ppsx, ppsm, pps	Diaporama PowerPoint
ppam, ppa	Complément PowerPoint
odp	Équivalent de PowerPoint dans OpenOffice
VSD, VSS, VST, VSW, VDX, VSX, VTX, VSDX, VSDM, VSSX, VSSM, VSTX, VSTM, VSL	Document Visio
pub	Document Publisher
txt	Fichier texte

Format de fichier (extension)	Description du format de fichier
mht, mhtml, htm, html	Page Web
rtf	Document écrit
pdf	Fichier de document portable
xps	Fichier semblable à un PDF
msg	Courriel Outlook
oft	Modèle Outlook
wps	Document Works
one	Fichier OneNote
accdb, accdt, mdb	Base de données Access
xml	Fichier texte qui peut être ouvert dans presque tous les programmes
mp4, wmv, MPG, MP2, MPEG,	Fichier vidéo
mp3, dss	Fichier audio
gif, jpg, png, tif, bmp, wmf, emf, svg, webp	Fichier image
zip	Fichier compressé
tmx	Fichier de mémoire de traduction
tbx	Fichier de données terminologiques (glossaire)

14 APPENDICE G – SÉCURITÉ ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

14.1 FAMILLES DE CONTRÔLES SELON L'ITSG-33

Le PCS est constitué de contrôles de sécurité définis par le Centre de la sécurité des télécommunications (CST).

Ces contrôles sont répertoriés dans le document d'orientation ITSG-33 du CST, intitulé La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie.

Ces contrôles de sécurité sont divisés en trois classes : contrôles de sécurité techniques, contrôles de sécurité opérationnels et contrôles de sécurité de gestion.

Ces trois classes sont elles-mêmes subdivisées en dix-sept (17) familles :

Classes	Contrôles de sécurité techniques	Contrôles de sécurité opérationnels	Contrôles de sécurité de gestion
Familles	AC – Contrôle d'accès	AT – Sensibilisation et formation	CA – Évaluation de sécurité et autorisation
	AU – Vérification et responsabilité	CM – Gestion des configurations	PL – Planification
	IA – Identification et authentification	CP – Planification d'urgence	RA – Évaluation des risques
	SC – Protection des systèmes et des communications	IR – Intervention en cas d'incident	SA – Acquisition des systèmes et des services
		MA – Maintenance	
		MP – Protection des supports	
		PE – Protection physique et environnementale	
		PS – Sécurité du personnel	
		SI – Intégrité de l'information et des systèmes	

14.1.1 Contrôles de sécurité de l'ITSG-33 appliqués au SGDSL

Les contrôles de sécurité définis pour la solution du SGDSL sont fondés sur les contrôles figurant dans l'ITSG-33 et sont présentés ci-dessous. Pour chacun des contrôles du SGDSL, le code correspondant de l'ITSG-33 est indiqué.

Le tableau ci-dessous dresse la liste des familles de contrôles de sécurité de l'ITSG-33 qui sont utilisées.

Famille de contrôles	Description	Sigle
Contrôle d'accès	Contrôles permettant d'autoriser ou d'interdire l'accès d'un utilisateur aux ressources dans le système d'information	AC
Vérification et responsabilité	Contrôles permettant de recueillir, d'analyser et de stocker les enregistrements de vérification associés aux opérations utilisateur exécutées dans le système d'information.	AU
Gestion des configurations	Contrôles permettant la gestion et le contrôle de tous les composants du système d'information (p. ex., éléments matériels, logiciels et de configuration).	CM
Planification d'urgence	Contrôles permettant d'assurer la disponibilité des services du système d'information dans l'éventualité d'une panne de composant ou d'un désastre.	CP
Identification et authentification	Contrôles permettant de vérifier l'identification unique et l'authentification des utilisateurs qui tentent d'accéder aux ressources du système d'information.	IA
Intervention en cas d'incident	Contrôles permettant de détecter et de signaler les incidents de sécurité liés au système d'information, et d'intervenir.	IR
Protection des supports	Contrôles permettant de protéger les supports du système d'information (p. ex., disques et bandes) tout au long de leur cycle de vie.	MP
Sécurité du personnel	Contrôles servant à appliquer les procédures nécessaires afin de veiller à ce que tout le personnel ayant accès au système d'information possède les autorisations requises ainsi que les niveaux d'habilitation appropriés.	PS
Protection physique et environnementale	Contrôles liés à l'accès physique à un système d'information et à la protection de l'équipement environnemental auxiliaire (c.-à-d. alimentation, climatisation, câblage) servant à son exploitation.	PE
Évaluation des risques	Contrôles qui concernent l'exécution des évaluations des risques et de l'analyse des vulnérabilités.	RA
Sensibilisation et formation	Contrôles qui concernent la formation des utilisateurs sur la sécurité du système d'information.	AT
Protection des systèmes et des communications	Contrôles permettant de protéger le système d'information lui-même ainsi que ses communications internes et externes.	SC
Intégrité de l'information et du système	Contrôles permettant de protéger l'intégrité des composants du système d'information et des données traitées par ce système.	SI
Maintenance	Contrôles permettant d'assurer la maintenance du système d'information et sa disponibilité permanente.	MA
Acquisition des systèmes et des services	Contrôles qui concernent la passation de marchés pour l'acquisition des produits et des services nécessaires à la mise en œuvre et à l'exploitation du système d'information. ***	SA

Numéros des exigences en matière	Profil de contrôle de sécurité (PCS)	Description	FedRAMP Nº d'identification

de sécurité aux fins du Canada uniquement			du contrôle de sécurité (NIST 800-53) Mise en correspondance des références (à titre informatif seulement)
SR-1	Contrôle d'accès	L'entrepreneur doit : a) élaborer, diffuser et examiner et mettre à jour chaque année les politiques sur le contrôle d'accès et les exigences connexes pour les composantes de l'infrastructure du **SGDSL**; b) fournir au BT les procédures de sécurité opérationnelles qui définissent les rôles et les responsabilités opérationnels en matière de contrôle d'accès. Éléments de preuve : a) Nom de l'instrument de politique : *Politique relative à la sécurité du SGDSL*, section 4 – Contrôle d'accès, pages 55 à 63. b) Sous-sections sur le contrôle d'accès : 4.1 – Portée; 4.2 – Calendrier de mise à jour et de renouvellement de la politique; 4.3 – Rôles et responsabilités; 4.4 – Gouvernance en matière de CA; 4.5 – Coordination entre les organisations; 4.6 – Mise en œuvre du CA; 4.7 – Gestion des comptes.	CA-1
SR-2	Contrôle d'accès	Les services de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) devraient créer automatiquement des comptes d'utilisateur et des comptes génériques pour la solution du SGDSL, c'est-à-dire : a) Attribuer un compte et un nom d'affichage uniques pour la solution du SGDSL, conformément à la norme définie dans l'énoncé des travaux, en appliquant les règles configurables de résolution de conflits et de désignation; b) Créer un compte sans privilège; c) Attribuer un mot de passe temporaire applicable au compte;	CA-2

		d) établir les attributs du compte et les privilèges de sécurité d'accès selon les directives du BT; e) communiquer le compte, le nom d'affichage et le mot de passe unique attribués pour la solution du SGDSL au demandeur du compte. (A) La solution du SGDSL devrait prendre en charge divers types de comptes, y compris ceux-ci : a) Comptes administratifs de l'entrepreneur (ou autres types de comptes de l'entrepreneur, au besoin); b) Comptes clients; c) Comptes d'utilisateur du BT; d) Comptes de gestion des utilisateurs du BT; e) Autres types de comptes (à définir lors de l'étape de l'adaptation des contrôles de sécurité) (B) Les comptes de gestion des utilisateurs devrait permettre la création, l'activation, la désactivation et la suppression de comptes d'utilisateur. (C) L'entrepreneur devrait mettre en œuvre des fonctions d'attribution de permissions au moyen de groupes et de rôles et permettre aux comptes de gestion des utilisateurs du BT d'attribuer ces permissions. (G) L'entrepreneur devrait fournir des fonctions de surveillance des comptes d'utilisateur. Ces fonctions doivent être accessibles aux comptes de gestion des utilisateurs. (L) La solution du SGDSL devrait créer un mot de passe temporaire à utilisation unique lors de la création d'un compte (ce mot de passe sera transmis à l'utilisateur au moyen d'un courriel sécurisé – à définir à l'étape de l'adaptation).	
SR-3	Contrôle d'accès	Le système devrait faire ce qui suit : a) Empêcher la réutilisation d'un compte de la solution du SGDSL selon les directives du BT; b) Autoriser les politiques de suspension de comptes, selon les directives du BT; c) Ne pas permettre l'accès à un compte suspendu; d) S'assurer qu'un compte suspendu n'envoie et ne reçoit aucun message lié au déroulement de travaux de la solution du SGDSL;	CA-2

		e) Interdire l'accès direct à l'infrastructure de service de la solution du SGDSL à partir de tout compte, selon les directives du BT.	
SR-4	Contrôle d'accès	L'entrepreneur devrait gérer les comptes d'opérateur de l'infrastructure de la solution du SGDSL, comme suit : a) En déterminant les types de comptes (p. ex., individuel, collectif, relatif à un système, à un appareil ou à une application, invité ou anonyme, et temporaire); b) En établissant les conditions d'adhésion à des groupes; c) En définissant les opérateurs autorisés de l'infrastructure de la solution du SGDSL et en précisant les droits d'accès; d) En demandant les approbations requises pour les demandes d'établissement de comptes; e) En sélectionnant un identifiant qui correspond uniquement à l'opérateur ou à l'appareil; f) En attribuant l'identifiant de l'opérateur à la partie visée ou l'identifiant d'appareil à l'appareil visé; g) En établissant, en activant, en modifiant, en désactivant et en supprimant les comptes; h) En autorisant et en surveillant précisément l'utilisation des comptes temporaires et des comptes d'invités et anonymes; i. En avisant l'administrateur des comptes lorsqu'un compte temporaire n'est plus requis et lorsque les opérateurs de la solution du SGDSL quittent leur emploi ou sont mutés, ou lorsque des changements sont apportés à l'utilisation de la solution du SGDSL ou selon le principe du besoin de connaître ou du besoin de partager; i) En veillant à ce que les identifiants ne soient pas réutilisés durant au moins un an; j) En désactivant : i. Les comptes temporaires qui ne sont plus nécessaires; ii. Les comptes des utilisateurs qui ont quitté leur emploi ou ont été mutés; iii. Les comptes après un certain nombre de jours d'inactivité, selon les directives du BT,	CA-2(2)

		iv. Les comptes temporaires et créés en cas d'urgence qui sont actifs depuis une période donnée; k) En attribuant l'accès à l'infrastructure de la solution du SGDSL en fonction de ce qui suit : i. Une autorisation d'accès valide; ii. L'utilisation prévue du système; iii. D'autres exigences de l'entrepreneur ou du BT; l) En examinant les comptes au moins une fois par mois; m) En verrouillant les comptes après dix (10) tentatives d'ouverture de session infructueuses dans un délai de cinq (5) minutes; n) En gardant les comptes verrouillés jusqu'à ce qu'ils soient déverrouillés manuellement par un autre opérateur.	
SR-5	Contrôle d'accès	La solution du SGDSL devrait journaliser les événements suivants : a) Création d'un compte; b) Modification d'un compte; c) Suspension d'un compte; d) Fermeture d'un compte; e) Suppression d'un compte; f) Consultation des comptes de la solution du SGDSL dont l'utilisateur n'est pas le principal responsable.	CA-2(4)
SR-6	Contrôle d'accès	L'infrastructure de la solution du SGDSL devrait appliquer les autorisations d'accès des opérateurs.	CA-3
SR-7	Contrôle d'accès	Le système d'information de la solution du SGDSL devrait appliquer les autorisations d'accès des opérateurs ne doit pas divulguer d'information hors des limites établies du système à moins d'utiliser des mesures de protection et des procédures pour valider le caractère approprié de l'information à divulguer.	CA-3(9)
SR-8	Contrôle d'accès	L'entrepreneur devrait veiller à la séparation des tâches des opérateurs, au besoin, afin de prévenir toute activité malveillante et toute collusion, en fonction du profil d'accès attribué à l'opérateur selon son rôle. L'entrepreneur devrait définir la séparation des tâches.	CA-5
SR-9	Contrôle d'accès	L'entrepreneur devrait mettre en œuvre une politique de privilège minimum à l'égard des utilisateurs de l'infrastructure de la solution du SGDSL, comme suit : a) Configurer les mécanismes de contrôle d'accès de manière à accorder le privilège minimum, c.-à-d. En ne donnant aux opérateurs (et aux	CA-6

		processus exécutés en leur nom) que l'accès dont ils ont besoin pour accomplir les tâches qui leur sont attribuées; b) Créer des comptes non privilégiés qui seront utilisés pour les tâches non opérationnelles; c) Limiter l'attribution de comptes super-utilisateur (p. Ex. Root) aux opérateurs désignés; d) Empêcher le partage des comptes des opérateurs; e) Identifier de manière distincte l'utilisateur qui a effectué chaque intervention sur l'infrastructure de service de la solution du SGDSL.re.	
SR-10	Contrôle d'accès	La solution du SGDSL doit : a) Afficher une bannière (définie au cours de l'étape d'adaptation) approuvée par le BT sur la page de connexion de toute application Web destinée aux utilisateurs. b) Inclure un mécanisme de contrôle de l'accès qui : i. Interdit l'accès aux composants et aux ressources de l'infrastructure de la solution du SGDSL sans l'identification, l'authentification et l'autorisation qui conviennent; ii. Affiche, au moment de la connexion, une bannière d'avertissement approuvée par le BT, que les utilisateurs autorisés doivent accepter avant d'obtenir l'accès aux composants de l'infrastructure de la solution du SGDSL; iii. Affiche, lorsque l'utilisateur ouvre une session (accède au système), la date et l'heure d'ouverture de sa session précédente; iv. Offre une option de déconnexion bien visible chaque fois qu'un utilisateur s'authentifie pour avoir accès aux composants de l'infrastructure de la solution du SGDSL. c) Inclure un mécanisme de verrouillage de session de l'opérateur qui : i. Bloque l'accès aux composants de l'infrastructure en verrouillant automatiquement la session de l'utilisateur après une période d'inactivité maximale de 60 minutes;	CA-8

		ii. Empêche l'accès aux composants de l'infrastructure en verrouillant la session de l'utilisateur à sa demande; iii. Affiche un économiseur d'écran qui ne contient aucune information importante et qui remplace tout le contenu précédemment affiché à l'écran lorsque la session de l'utilisateur est verrouillée; iv. Déverrouille la session de l'utilisateur lorsqu'il réussit à s'authentifier. d) Inclure un mécanisme de contrôle de l'accès qui : i. Interdit l'accès de l'utilisateur aux fonctions, aux composants et aux ressources de la solution du SGDSL sans l'identification, l'authentification et l'autorisation qui conviennent; ii. Affiche des renseignements sur l'utilisation du système approuvés par le BT que les utilisateurs doivent accepter avant d'obtenir l'accès à la solution du SGDSL; iii. Affiche, lorsque l'utilisateur ouvre une session (accède au système), la date et l'heure d'ouverture de sa session précédente; iv. Offre une option de déconnexion bien visible chaque fois qu'un utilisateur s'authentifie pour avoir accès à la solution du SGDSL. e) Afficher une description des utilisations autorisées du système. f) Afficher le niveau de classification le plus élevé d'information que le système peut stocker et traiter (Protégé B).	
SR-11	Contrôle d'accès	L'entrepreneur devrait s'assurer que les opérateurs qui ont recours à la télégestion de la solution du SGDSL utilisent une méthode approuvée par le BT qui respecte les conditions suivantes : a) Gestion à distance limitée à l'infrastructure de la solution du SGDSL située à l'intérieur d'un point de prestation de services de l'entrepreneur, au moyen de consoles de gestion dédiées au SGDSL; b) Consignation des méthodes autorisées de gestion à distance, ainsi que des restrictions d'utilisation et des lignes directrices de mise en œuvre pour chacune de ces méthodes;	CA-17

		c) Surveillance aux fins de détection des cas de gestion à distance non autorisée; d) Autorisation de la télégestion avant de permettre la connexion; e) Utilisation de mécanismes automatiques pour faciliter la surveillance et le contrôle des méthodes de télégestion; f) Acheminement des composantes d'infrastructure de la solution du SGDSL par l'intermédiaire d'un nombre limité de points de contrôle d'accès gérés; g) Protection de l'information sur les mécanismes de télégestion contre l'utilisation et la divulgation non autorisées; h) Utilisation de mécanismes automatiques pour faciliter la surveillance et le contrôle des méthodes de télégestion. L'entrepreneur devrait fournir des mécanismes sécurisés d'accès à distance (hors des réseaux du GC) pour les utilisateurs qui n'ont pas déjà un accès sécurisé à distance aux réseaux du GC.	
SR-12	Contrôle d'accès	L'entrepreneur doit établir des politiques et des procédures qui appuient les processus opérationnels et mettre en œuvre des mesures techniques afin de protéger ***La solution SGDSL*** dans des environnements de réseau sans fil, notamment comme suit : a) Mise en œuvre et configuration de pare-feu du périmètre de manière à restreindre le trafic non autorisé; b) Paramètres de sécurité permettant un chiffrement efficace aux fins d'authentification et de transmission, conformément à l'ITSP.40.111 du CST visant les données de niveau Protégé B; c) Renforcement de la sécurité en remplaçant les paramètres par défaut du fournisseur (p. ex., clés de cryptage, mots de passe et chaînes de la communauté du protocole SNMP); d) Accès des utilisateurs, y compris les utilisateurs d'appareils de réseau sans fil, limité au personnel autorisé; e) Capacité de détecter la présence d'appareils non autorisés (indésirables) dans le réseau sans fil afin de les débrancher rapidement du réseau.	CA-18
SR-13	Contrôle d'accès	L'entrepreneur devrait mettre en œuvre une politique sur les appareils mobiles applicable au SGDSL. Cette politique devrait comprendre au minimum ce qui suit :	CA-19

		a) Formation sur la sensibilisation aux logiciels malveillants propres aux appareils mobiles. Cette formation doit faire partie de la formation sur la sensibilisation à la sécurité de l'information de l'entrepreneur; b) Liste documentée des boutiques d'applications approuvées pour les appareils mobiles qui permettent d'accéder aux données gérées par les fournisseurs et de les stocker; c) Politique documentée interdisant l'installation d'applications non approuvées ou d'applications approuvées qui n'ont pas été obtenues par l'intermédiaire d'une boutique d'applications déterminée à l'avance; d) Le cas échéant, énoncé clair, dans la politique « apportez votre équipement personnel de communication » (AVEC) et la formation de soutien sur la sensibilisation, concernant les applications, les boutiques d'applications et les extensions et modules d'extension des applications approuvés qui peuvent être utilisés dans le cadre de la politique AVEC; e) Politique documentée relativement aux applications mobiles, qui comprend une définition écrite des applications mobiles ainsi que de l'utilisation et des exigences acceptables pour tous les appareils mobiles. L'entrepreneur doit publier et communiquer la politique et les exigences en question dans le cadre du programme de sensibilisation et de formation à la sécurité de l'entreprise; f) Approbation préalable des services infonuagiques utilisés par les appareils mobiles de l'entreprise ou dans le cadre de la politique AVEC pour l'utilisation et le stockage des données opérationnelles liées au SGDSL; g) Processus documenté de validation des applications afin de vérifier les problèmes de compatibilité liés aux appareils mobiles, au système d'exploitation et aux applications; h) Définition dans la politique AVEC des appareils et des exigences d'admissibilité afin de permettre l'utilisation des appareils aux termes de cette politique; i) Tenue à jour un répertoire de tous les appareils mobiles utilisés pour stocker les données du SGDSL et y avoir accès;	

		j) Inclusion, pour chaque appareil figurant dans le répertoire, des détails sur tous les changements apportés à l'état de ces appareils (p. ex., le système d'exploitation et les niveaux de correction, les états des appareils perdus ou mis hors service, les personnes à qui les appareils sont attribués et les appareils approuvés dans le cadre de la politique AVEC); k) Déploiement d'une solution centralisée de gestion des appareils mobiles pour tous les appareils mobiles autorisés à stocker, à transmettre ou à traiter les données du SGDSL; l) Exigence dans la politique sur les appareils mobiles concernant l'utilisation du chiffrement pour l'ensemble de l'appareil ou pour les données de nature délicate de tous les appareils mobiles et application de cette exigence au moyen de contrôles technologiques; m) Interdiction dans la politique sur les appareils mobiles du contournement des contrôles de sécurité intégrés des appareils mobiles (p. ex. débridage ou racinement) et application de l'interdiction au moyen de contrôles de détection et de prévention sur l'appareil ou au moyen d'un système centralisé de gestion des appareils (p. ex. gestion des appareils mobiles); n) Clarification dans la politique AVEC, s'il y a lieu, des attentes en matière de protection des renseignements personnels, des exigences en matière de litiges, de découverte électronique et de réserves juridiques. Par ailleurs, la politique AVEC devrait clairement énoncer les attentes au sujet de la perte de données opérationnelles non liées au SGDSL s'il faut écraser les données de l'appareil; o) Configuration des appareils visés par la politique AVEC et des appareils appartenant à l'entrepreneur de manière à nécessiter un écran de verrouillage automatique. Cette exigence devrait être appliquée au moyen de contrôles techniques; p) Gestion des changements apportés aux systèmes d'exploitation, aux niveaux de correctifs et aux applications des appareils mobiles dans le cadre du processus de gestion du changement de l'entrepreneur;	

		q) Documentation des politiques relatives aux mots de passe, qui s'appliquent aux appareils mobiles, et application de ces politiques au moyen de contrôles techniques sur tous les appareils appartenant à l'entrepreneur ou les appareils approuvés aux fins de la politique AVEC. Ces politiques devrait interdire la modification de la longueur du mot de passe ou du NIP ainsi que des exigences en matière d'authentification; r) Politique sur les appareils mobiles qui exige que les utilisateurs d'appareils visés par la politique AVEC doivent faire des copies de sauvegarde des données, qui interdire l'utilisation de boutiques d'applications non approuvées et qui exige l'utilisation de programmes de protection contre les logiciels malveillants (lorsque de tels programmes sont pris en charge); s) Exigence que les appareils mobiles qui peuvent être utilisés dans le cadre du programme AVEC de l'entrepreneur ou les appareils mobiles attribués devrait permettre au responsable ministériel de la TI de l'entrepreneur d'effectuer un nettoyage à distance ou faire en sorte que toutes les données fournies par une entreprise soient nettoyées par le responsable ministériel de la TI de l'entrepreneur; t) Exigence que les appareils mobiles qui permettent de se connecter aux réseaux de l'entrepreneur ou de stocker des renseignements sur l'entreprise et d'y avoir accès devrait permettre de valider à distance les versions ou les correctifs du logiciel; u) Exigence que tous les appareils mobiles devrait appliquer les plus récents correctifs de sécurité installés lorsque le fabricant ou le transporteur de l'appareil les rend disponibles de façon générale. Le personnel autorisé de la TI devrait être en mesure d'appliquer ces mises à jour à distance; v) Précision dans la politique AVEC des systèmes et des serveurs qui peuvent être utilisés avec un appareil visé par la politique AVEC ou auxquels l'appareil peut accéder.	
SR-14	Contrôle d'accès	L'entrepreneur devrait obtenir l'approbation du BT concernant l'utilisation (accès, traitement, stockage ou transmission d'information) de systèmes d'information	CA-20

		externes (à l'entrepreneur) pour la fourniture du SGDSL.	
SR-15	Contrôle d'accès	L'entrepreneur devrait restreindre l'utilisation des supports de données portatifs (p. ex., clés USB) contrôlés par l'entrepreneur dans le cadre de la solution du SGDSL, comme suit : a) Limiter l'utilisation aux opérateurs autorisés seulement; b) Limiter l'utilisation aux composantes de l'infrastructure du SGDSL. La sélection et l'utilisation de supports de données portatifs doit être conforme à l'AMPTI 2014-01 du SCT.	CA-20(2)
SR-16	Sensibilisation et formation sur la sécurité	L'entrepreneur devrait fournir au BT des politiques et des procédures de sécurité opérationnelle de la solution du SGDSL qui comprennent les rôles et les responsabilités opérationnelles en matière de sensibilisation et de formation sur la sécurité. L'entrepreneur devrait examiner et actualiser la politique (au moins aux trois ans) et les procédures (au moins chaque année) de sensibilisation et de formation sur la sécurité et fournir les résultats aux BT.	SF-1
SR-17	Sensibilisation et formation sur la sécurité	L'entrepreneur devrait sensibiliser les utilisateurs de l'infrastructure des services de la solution du SGDSL à la sécurité et leur donner une formation en la matière, dans les circonstances suivantes : a) Dans le cadre de la formation initiale aux nouveaux opérateurs; b) Avant d'accorder un accès à l'infrastructure à l'infrastructure de la solution du SGDSL ou avant l'exécution des tâches attribuées; c) Chaque année ou lorsque des changements concernant la sécurité sont apportés à la solution du SGDSL.	SF-2, SF-3
SR-18	Sensibilisation et formation sur la sécurité	L'entrepreneur devrait surveiller et documenter la sensibilisation et la formation en matière de sécurité des opérateurs de l'infrastructure du SGDSL, y compris ce qui suit : a) Consigner la date des cours et le nom des participants à chaque cours de formation; b) Conserver les documents pour les trois (3) dernières années.	SF-4
SR-19	Vérification et responsabilité	L'entrepreneur devrait présenter au BT les procédures opérationnelles de sécurité relatives au SGDSL qui définissent les rôles et les responsabilités opérationnels en matière de vérification et de responsabilité. L'entrepreneur devrait, au moins une fois chaque année, examiner et actualiser les procédures qui	VR-1

		définissent les rôles et les responsabilités opérationnels en matière de vérification et de responsabilité.	
SR-20	Vérification et responsabilité	Les services de gestion de l'identité, des justificatifs d'identité et de l'accès de la solution du SGDSL devrait journaliser les événements ci-dessous conformément aux exigences en matière de journalisation pour le niveau d'assurance 3 (LOA3) de l'ITSP.30.031 V3 (https://www.cse-cst.gc.ca/fr/node/1842/html/26717) : a) Événements d'authentification réussis; b) Événements d'authentification non réussis.	VR-2
SR-21	Vérification et responsabilité	L'entrepreneur devrait : a) Examiner et mettre à jour la liste des événements vérifiables pour la solution du SGDSL au moins une fois tous les 180 jours ouvrables; b) Inclure l'exécution des fonctions privilégiées dans la liste des événements de vérification; c) Consigner les événements désignés et approuvés par le BT; d) Générer automatiquement des alertes en temps réel (p. ex., à l'aide de règles de corrélation) à la suite d'indications de compromission et de compromission potentielle.	VR-2(3)
SR-22	Vérification et responsabilité	L'entrepreneur devrait s'assurer que la solution du SGDSL répond aux exigences suivantes : a) Préparer, selon la définition du BT, des dossiers de vérification permettant, au minimum, d'établir ce qui suit : i. Le type d'événement; ii. La date et l'heure de l'événement; iii. L'endroit où l'événement a eu lieu, la source de l'événement; iv. Le résultat (réussite ou échec) de l'événement; v. L'identité de tout utilisateur ou de toute personne associés à l'événement; b) Classer les événements de vérification par type, lieu ou sujet; c) Gérer le contenu des dossiers de vérification générés.	VR-3
SR-23	Vérification et responsabilité	L'entrepreneur devrait gérer la capacité de stockage des dossiers de vérification relatifs à la solution du SGDSL, en faisant ce qui suit :	VR-4, VR-5(1)

		a) Attribuer une capacité de stockage suffisante pour les dossiers de vérification (à définir au cours du processus d'adaptation); b) Configurer la vérification de manière à empêcher le dépassement de la capacité de stockage; c) Avertir le centre des opérations lorsque le volume de stockage des dossiers de vérification atteint 75 % de la capacité de stockage; d) Écraser les dossiers de vérification les plus anciens si la capacité maximale est atteinte.	
SR-24	Vérification et responsabilité	La fonction de vérification de la solution du SGDSL devrait réagir aux défaillances en matière de vérification, comme suit : a) En avisant le centre des opérations et le BT (pour les événements de vérification à définir au cours du processus d'adaptation; b) En écrasant les dossiers de vérification les plus anciens si la capacité maximale de stockage est atteinte.	VR-5
SR-25	Vérification et responsabilité	Afin de générer l'horodatage des dossiers de vérification, la solution du SGDSL devrait synchroniser les horloges internes avec les horloges d'une source faisant autorité et approuvée par le BT.	VR-8, VR-8(1)
SR-26	Vérification et responsabilité	La solution du SGDSL devrait : a) Protéger les renseignements de vérification contre l'accès, les modifications et la suppression non autorisés; b) Sauvegarder les dossiers de vérification dans un système ou un support différent de celui dont la vérification est prévue selon un calendrier précisé par le BT.	VR-9, VR-9(1), VR-9(2), VR-9(3), VR-9(4)
SR-27	Évaluation et autorisation de sécurité	L'entrepreneur devrait effectuer des évaluations des vulnérabilités : a) Avant la mise en production de la solution du SGDSL; b) Au moins une fois par année; c) Lorsqu'il y a des changements importants qui pourraient avoir une incidence sur la sécurité du système. À la fin de l'évaluation des vulnérabilités, l'entrepreneur devrait élaborer un plan d'atténuation des vulnérabilités, approuvé par le BT, pour ***La solution SGDSL*** conformément à l'énoncé des travaux. Le plan devrait comprendre des mesures de protection pour atténuer les risques cernés dans le cadre de l'évaluation des vulnérabilités.	CE-7(2)

SR-28	Gestion de la configuration	L'entrepreneur devrait définir, consigner et gérer de manière continue une configuration de référence courante des composants de l'infrastructure du SGDSL, en plus de conserver les deux (2) versions précédentes.	GC-2, GC-2(1), GC-2(2), GC-2(3), GC-2(4)
SR-29	Gestion de la configuration	L'entrepreneur devrait permettre uniquement l'exécution des logiciels autorisés qu'il a lui-même définis et qui ont obtenu l'approbation CU, dans le cadre de la solution du SGDSL.	GC-2(5)
SR-30	Gestion de la configuration	L'entrepreneur devrait : a) Planifier et mettre à l'essai la mise en œuvre des logiciels, du matériel et des documents nouveaux et modifiés en vue de lancer la solution du SGDSL sans utiliser l'environnement de production ou l'environnement d'essais contrôlés du SGDSL; b) Planifier et mettre à l'essai la mise en œuvre des logiciels, du matériel et des documents nouveaux et modifiés en vue de lancer solution du SGDSL de la manière approuvée par le BT; c) Élaborer et mettre en œuvre des procédures de distribution, d'installation et d'annulation des changements apportés en vue du lancement de la solution du SGDSL.	GC-3(2), GC-3(3), GC-3(4)
SR-31	Gestion de la configuration	L'entrepreneur devrait évaluer les répercussions des changements sur la sécurité, comme suit : a) Analyse des nouveaux logiciels avant leur installation dans un environnement opérationnel afin de déterminer les répercussions sur la sécurité attribuables aux failles, aux points faibles, à l'incompatibilité ou à la malveillance intentionnelle; b) Communication au bt de l'incidence possible sur la sécurité des changements avant leur mise en œuvre; c) Vérification des fonctions de sécurité après les changements pour s'assurer qu'elles ont été mises en œuvre correctement, fonctionnent comme prévu et produisent les résultats souhaités quant au respect des exigences pertinentes en matière de sécurité.	GC-4
SR-32	Gestion de la configuration	L'entrepreneur devrait vérifier les changements apportés au système d'information, au moins tous les douze mois et lorsque les circonstances le justifient, pour déterminer si des changements non autorisés ont été apportés.	GC-4
SR-33	Gestion de la configuration	L'entrepreneur devrait passer en revue chaque trimestre les privilèges de l'opérateur du SGDSL.	GC-5(5)

SR-34	Gestion de la configuration	L'entrepreneur devrait utiliser des mécanismes automatiques pour la gestion, l'application et la vérification centralisées des paramètres de configuration de la solution du SGDSL, y compris les produits d'autres fournisseurs inclus dans la solution. Les divergences par rapport aux paramètres de configuration établis devrait être cernées et consignées. L'entrepreneur devrait surveiller et gérer les modifications aux paramètres de configuration.	GC- 6, GC-6(1), GC-6(2)
SR-35	Gestion de la configuration	L'entrepreneur devrait créer un dossier d'incident de sécurité lorsqu'un changement non autorisé à la configuration est relevé dans ***La solution SGDSL***.	GC-6(3)
SR-36	Gestion de la configuration	a) L'entrepreneur devrait configurer la solution du SGDSL pour fournir seulement les fonctions essentielles : les fonctions non essentielles devrait être désactivées. b) L'entrepreneur interdit expressément ou restreint l'utilisation des fonctions, ports, protocoles ou services suivants : [à définir lors du processus d'adaptation, avec l'approbation du BT]. c) L'entrepreneur examine mensuellement le système d'information pour déceler et éliminer les fonctions, ports, protocoles ou services non nécessaires. d) L'entrepreneur désactive dans la solution du SGDSL les fonctions, les ports, les protocoles et les services estimés non nécessaires ou non sécuritaires. e) L'entrepreneur utilise un processus d'inscription pour s'assurer de la gestion, du suivi et de la surveillance du système est des fonctions, ports, protocoles et services mis en œuvre, et prend les mesures pour assurer la conformité à ce processus. f) L'entrepreneur utilise un processus pour déterminer les composantes dont l'exécution est autorisée dans la solution du SGDSL et utiliser un mécanisme de refus systématique et autorisation par exception pour permettre l'exécution des composantes autorisées; l'entrepreneur examine et met à jour la liste des composantes autorisées.	GC- 7, GC-7(1), GC-7(2), GC-7(3), GC-7(5)
SR-37	Gestion de la configuration	L'entrepreneur devrait élaborer et tenir un répertoire des composantes de la solution du SGDSL qui : a) Reflète fidèlement la configuration actuelle des composantes;	GC-8, GC-8(1)

		b) Respecte le niveau de précision jugé nécessaire au suivi et à l'établissement des rapports; c) Comprend les renseignements jugés nécessaires pour assurer une responsabilisation efficace à l'égard des biens; d) Est accessible aux fins d'examen et de vérification par le bt; e) Est mis à jour en tant que partie intégrante des installations de composantes, des suppressions et des mises à jour de la solution du sgdsl.	
SR-38	Gestion de la configuration	L'entrepreneur devrait fournir un plan de gestion de la configuration pour la solution du SGDSL qui : a) Décrit les rôles et les responsabilités ainsi que les processus et les procédures de gestion de la configuration; b) Définit les éléments de configuration de la solution du SGDSL et le moment où ces éléments sont soumis au processus de gestion de la configuration; c) Définit les moyens de détermination des éléments de configuration tout au long du cycle de vie de développement du système ainsi que le processus de gestion de la configuration de ces éléments; d) Définit les processus de gestion des correctifs pour les logiciels personnalisés utilisés dans la solution du SGDSL, y compris ce qui suit : i. La détection, le signalement et la correction des failles des logiciels personnalisés; ii. La mise à l'essai des mises à jour destinées à corriger les failles afin d'en déterminer l'efficacité et les éventuels effets sur les services liés à la solution du SGDSL avant de procéder à leur installation; iii. L'incorporation de la correction des failles dans le processus de gestion de la configuration pour la solution du SGDSL; e) Définit les processus de gestion des correctifs des composants de la solution du SGDSL, ce qui comprend : i. L'utilisation de la version à jour des applications et des systèmes d'exploitation, ii. Le fait de veiller à ce que les vulnérabilités soient évaluées et à ce que les correctifs de sécurité fournis par le fournisseur soient appliqués rapidement;	GC-9, GC-9(1)

		iii. L'établissement de l'ordre de priorité des correctifs critiques à l'aide d'une approche fondée sur le risque; iv. La mise hors ligne et la remise en ligne des applications; v. L'harmonisation des niveaux de criticité avec les correctifs, selon les directives du BT; vi. L'attribution d'une cote aux vulnérabilités conformément à la version 3 du Common Vulnerability Scoring System (CVSS); vii. L'utilisation d'une méthode de mise à l'essai et de vérification pour s'assurer que les correctifs sont mis en œuvre correctement; viii. Aviser le BT des vulnérabilités liées à la configuration qui permettraient à une personne non autorisée de compromettre la confidentialité, l'intégrité ou la disponibilité de la solution du SGDSL.	
SR-39	Gestion de la configuration	L'entrepreneur devrait fournir au BT un processus de gestion des changements où il décrit : a) Les pouvoirs de l'entrepreneur en matière de gestion du changement; b) Les rôles et les responsabilités des ressources de l'entrepreneur en matière de gestion du changement; c) La façon dont l'entrepreneur utilisera le processus de gestion du changement pour faciliter l'élaboration de la solution du SGDSL (p. ex., concept des opérations);	GC-9, GC-9(1)
SR-40	Planification d'urgence	(A) L'entrepreneur devrait élaborer, consigner et diffuser, à l'interne et au BT, ce qui suit : a) Les procédures de planification d'urgence pour ***La solution SGDSL*** qui préciser précisant le but, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et les mesures d'assurance de la conformité; b) Les procédures pour faciliter la mise en œuvre des mesures de contrôle associées à la planification d'urgence. c) L'entrepreneur devrait examiner et mettre à jour les procédures de planification d'urgence conformément à l'énoncé des travaux.	PU-1, PU-2
SR-41	Planification d'urgence	L'entrepreneur devrait, en collaboration avec le BT, établir les priorités nationales en matière de restauration pour ce qui est de la solution du SGDSL	PU-7, PU-8

		selon leur ordre de préséance, conformément aux directives du BT.	
SR-42	Planification d'urgence	L'entrepreneur devrait : a) Effectuer des sauvegardes des données des utilisateurs contenues dans le système d'information (sauvegarde quotidienne incrémentielle, sauvegarde hebdomadaire complète); b) Effectuer des sauvegardes des données du système contenues dans le système d'information (sauvegarde quotidienne incrémentielle, sauvegarde hebdomadaire complète); c) Effectuer des sauvegardes des documents d'information du système, y compris les documents sur la sécurité (sauvegarde quotidienne incrémentielle, sauvegarde hebdomadaire complète); d) Protéger la confidentialité, l'intégrité et l'accessibilité de l'information de sauvegarde aux sites de stockage; e) Examiner les données de sauvegarde de la solution du sgdsl chaque mois afin de vérifier la fiabilité des supports et l'intégrité des données; f) Utiliser un échantillon de données de sauvegarde de la solution du sgdsl lors de la restauration des fonctions de ce dernier, dans le cadre de la mise à l'essai du plan de continuité des services.	PU-9, PU-9(1), PU-9(2)
SR-43	Planification d'urgence	L'entrepreneur devrait conserver des copies de sauvegarde des logiciels du système d'exploitation et d'autres logiciels essentiels du système, ainsi que des copies de l'inventaire des composants dans une installation distincte ou dans un conteneur ignifuge, non situé dans l'immeuble où se trouve l'infrastructure de la solution du SGDSL.	PU-9(3)
SR-44	Planification d'urgence	L'entrepreneur devrait restaurer la solution du SGDSL selon un état précédent connu après une interruption, une compromission ou une panne.	PU-10
SR-45	Identification et authentification	a) L'entrepreneur devrait présenter au BT des procédures opérationnelles de sécurité qui définissent les rôles et les responsabilités opérationnels en vue de satisfaire aux exigences en matière d'identification et d'authentification énoncées dans le présent énoncé des travaux. b) L'entrepreneur devrait examiner et mettre à jour les procédures d'identification et	IA-1

		d'authentification conformément à l'énoncé des travaux.	
SR-46	Identification et authentification	La solution du SGDSL devrait : a) Identifier et authentifier de manière unique les opérateurs (ou les processus fonctionnant au nom des opérateurs) ; b) Attribuer un nom d'utilisateur et un mot de passe pour les comptes qui respectent les exigences de l'assurance de niveau 2 décrites dans la version 3 du document ITSP.30.031 ; c) Permettre la sélection d'une question pour la récupération du mot de passe ; d) Prévoir des mots de passe temporaires à utilisation unique pour l'inscription et la récupération de mots de passe; e) Prévoir des mots de passe temporaires à utilisation unique suffisamment aléatoires pour être imprévisibles et associés à une période de validité configurable précisée par le BT; f) Permettre l'envoi d'avis automatiques indiquant l'expiration prochaine du mot de passe, selon les directives du BT; g) Prévoir des politiques et des processus de récupération de mots de passe; h) Authentifier tout accès du client aux logiciels de la solution du SGDSL.	IA-2
SR-47	Identification et authentification	La solution du SGDSL devrait utiliser l'authentification multifactorielle pour l'accès au réseau au moyen de comptes privilégiés.	IA-2(1)
SR-48	Identification et authentification	L'infrastructure de la solution du SGDSL devrait : a) Effectuer une authentification multifactorielle au moyen jeton cryptographique matériel pour tous les comptes des opérateurs, conformément au niveau d'assurance 4 décrit dans la version 3 du document ITSP.30.031 (https://www.cse-cst.gc.ca/fr/node/1842/html/26717); b) Effectuer une authentification mutuelle des appareils mobiles d'opérateurs qui sont connectés au réseau et accepter uniquement les appareils mobiles d'opérateurs autorisés. Les appareils portatifs de stockage de données autorisés devraient être protégés par mot de passe (saisi sur l'appareil) ou munis d'un contrôle d'accès biométrique et les renseignements stockés devrait être chiffrés au moyen d'un programme certifié dans le	IA-3, IA-3(1), exigence spécifique du document ITSG-33 du CSTC : IA-2(100)

		cadre du Programme de validation des modules cryptographiques (PVMC) qui fonctionne sur l'appareil lui-même.	
SR-49	Identification et authentification	L'entrepreneur devrait gérer les comptes des utilisateurs de l'infrastructure de la solution du SGDSL de la manière suivante : a) Détermination des types de comptes (de personne, de groupe, de système, d'appareil, d'application, d'invité ou anonyme, temporaire); b) Etablissement des conditions d'appartenance à un groupe; c) Détermination des utilisateurs autorisés de l'infrastructure de la solution du SGDSL et de leurs privilèges d'accès; d) Obtention des approbations nécessaires avant de traiter des demandes de création de comptes; e) Sélection d'un identificateur qui désigne de façon unique l'utilisateur ou l'appareil; f) Attribution de l'identificateur de l'utilisateur à la personne ou au groupe visé ou de l'identificateur de l'appareil à l'appareil visé; g) Création, activation, modification, désactivation et suppression de comptes; h) Autorisation et surveillance de l'utilisation des comptes d'invité, anonymes et temporaires; i) Avis à l'administrateur des comptes lorsqu'un compte temporaire n'est plus requis et lorsque les opérateurs de la solution du SGDSL quittent leur emploi ou sont mutés, ou lorsque des changements sont apportés à l'utilisation de la solution du SGDSL ou selon le principe du besoin de connaître ou du besoin de partager; j) Prévention de la réutilisation des identificateurs pendant au moins un an; k) Désactivation : i. Des comptes temporaires qui ne sont plus nécessaires; ii. Des comptes des utilisateurs qui ont quitté leur emploi ou ont été mutés; iii. Des comptes après un certain nombre de jours d'inactivité, selon les directives du BT; iv. Des comptes temporaires et créés en cas d'urgence qui sont actifs depuis une période donnée;	IA-4

		l) Attribution de l'accès à l'infrastructure du SGDSL en fonction de ce qui suit : i. Une autorisation d'accès valide; ii. L'utilisation prévue du système; iii. D'autres exigences de l'entrepreneur ou du BT; m) Examen des comptes au moins une fois par mois; n) Verrouillage du compte après 10 tentatives infructueuses entreprises en 5 minutes; o) Maintien du verrouillage du compte jusqu'à ce qu'un autre opérateur le déverrouille manuellement. L'entrepreneur devrait fournir des mécanismes pour faire ce qui suit : a) Empêcher la réutilisation d'identificateurs de comptes d'utilisateur (sans limite de temps); b) Désactiver les identificateurs de comptes d'utilisateur après un certain nombre de jours d'inactivité (selon le type de compte d'utilisateur), conformément aux directives du BT.	
SR-50	Identification et authentification	Les services de GIJIA du SGDSL devraient consigner les événements suivants : a) Création de comptes; b) Modification d'un compte; c) Désactivation d'un compte; d) Fermeture d'un compte; e) Changement de mot de passe; f) Enregistrement de justificatifs d'identité; g) Récupération de mot de passe; h) Expiration de justificatifs. Les services de GIJIA du SGDSL devrait protéger le journal de vérification au moyen de contrôles d'accès et d'un mécanisme de détection des tentatives de modification non autorisées des données du journal (p. ex., en utilisant des signatures numériques).	VR-2(3), IA-4
SR-51	Identification et authentification	L'entrepreneur devrait gérer les authentifiants des opérateurs par les moyens suivants : a) Vérification de l'identité de la personne, au moment de l'attribution initiale des authentificateurs; b) Etablissement du contenu initial des authentificateurs définis par l'entrepreneur; c) Vérification des authentificateurs pour veiller à ce qu'ils soient suffisamment robustes pour l'utilisation prévue;	IA-5

		d) Elaboration et mise en œuvre de procédures administratives concernant la distribution initiale des authentificateurs, les authentificateurs perdus, endommagés ou compromis, ainsi que l'annulation des authentificateurs; e) Modification du contenu par défaut des authentificateurs à l'installation des composants de l'infrastructure des services de la solution du SGDSL; f) Etablissement de la durée de vie minimale et maximale ainsi que des conditions de réutilisation des authentificateurs; g) Modification ou actualisation des authentificateurs au moins tous les 180 jours; h) Protection du contenu des authentificateurs contre la divulgation et la modification non autorisées; i) Application obligatoire par les utilisateurs de mesures spécifiques de protection des authentificateurs.	
SR-52	Identification et authentification	La solution du SGDSL devrait inclure de qui suit : a) Une validation du chemin du certificat X.509; b) Une vérification de l'état de révocation du certificat X.509.	IA-5
SR-53	Identification et authentification	Dans le cadre de l'authentification par mot de passe, l'infrastructure du SGDSL doit assurer ce qui suit : a) Application d'un niveau minimal de complexité des mots de passe, qui doivent être sensibles à la casse et comporter au moins 15 caractères, dont une majuscule, une minuscule, un chiffre et un caractère spécial; b) Chiffrement des mots de passe transmis; c) Hachage des mots de passe stockés; d) Application d'une durée de vie maximale de 90 jours des mots de passe; e) Interdiction de la réutilisation des mots de passe pendant 10 générations.	IA-5(1)
SR-54	Identification et authentification	Les services de gestion de l'identité, des justificatifs d'identité et de l'accès de la solution du SGDSL devraient : a) Fournir à l'utilisateur une liste de vérification qui précise les règles que devrait respecter un mot de passe, et cocher ces règles à mesure qu'elles sont respectées lorsque l'utilisateur saisit son mot de passe; b) Communiquer à l'utilisateur les règles relatives aux mots de passe établies par le bt, dont :	IA-5(1)

		i. Le nombre minimal de caractères; ii. Le nombre minimal de majuscules et de minuscules; iii. Le nombre minimal de chiffres; iv. Le nombre minimal de caractères non alphanumériques, v. Les mots trouvés dans un dictionnaire (anglais et français canadiens), vi. L'historique de réutilisation des mots de passe; vii. La durée de vie maximale des mots de passe.	
SR-55	Identification et authentification	L'entrepreneur devrait exiger que le processus d'inscription permettant aux opérateurs de la solution du SGDSL de recevoir des identifiants ou des authentifiants soit réalisé en personne devant l'autorité d'enregistrement désignée avec l'autorisation d'un représentant désigné par le représentant de l'entrepreneur (p. ex. un superviseur).	IA-5(3)
SR-56	Identification et authentification	L'infrastructure de la solution du SGDSL ne devrait pas transmettre de mots de passe en texte clair sur aucun réseau.	IA-5(6)
SR-57	Identification et authentification	L'entrepreneur ne devrait pas permettre l'intégration d'authentifiants statiques non chiffrés dans les applications de l'infrastructure du SGDSL ou des scripts d'accès, ou le stockage d'authentifiants dans des touches de fonction.	IA-5(7)
SR-58	Identification et authentification	L'infrastructure de la solution du SGDSL devrait masquer les données d'authentification de l'opérateur ou de l'utilisateur (p. ex., en masquant le contenu des champs de mot de passe) pendant le processus d'authentification.	IA-6
SR-59	Identification et authentification	L'entrepreneur devrait définir un processus d'autorisation du personnel de maintenance, y compris ce qui suit : a) Tenue à jour d'une liste des organisations et du personnel responsables de la maintenance; b) Vérification pour s'assurer que le personnel qui procède à la maintenance de la solution du sgdsl du bt dispose des autorisations d'accès nécessaires; c) Désignation de membres du personnel disposant des autorisations d'accès requises pour superviser la maintenance lorsque le personnel de maintenance n'a pas ces autorisations.	IA-8
SR-60	Intervention en cas d'incident	L'entrepreneur devrait :	II-1

		a) Présenter au BT les procédures opérationnelles de sécurité qui définissent les rôles et les responsabilités opérationnels pour satisfaire aux exigences en matière d'intervention en cas d'incident précisées dans le présent énoncé des travaux.	
SR-61	Intervention en cas d'incident	L'entrepreneur devrait : a) Fournir un plan de continuité des services (PCS) qui comprend les rôles opérationnels et les responsabilités en matière de continuité des services; b) Mettre à l'essai le plan de continuité des services (processus, procédures, rôles, responsabilités, etc.), et présenter les résultats des essais au BT conformé à l'énoncé des travaux à la fin de la mise à l'essai de ce plan; c) Fournir au BT un PCS qui comprend ce qui suit : i. Un plan détaillé et des processus documentés pour la restauration du service de la solution du SGDSL; ii. Des renseignements détaillés sur le plan de communication établi entre le BT et ses fournisseurs; iii. Des plans et des processus détaillés de transfert des fonctions d'exploitation, de gestion et d'administration à un centre des opérations secondaire; iv. Des stratégies de sauvegarde pour les installations de centres de données, les installations réseau, les systèmes et les données de soutien opérationnel et les principales composantes de service; v. Les moyens que l'entrepreneur prendra pour s'assurer que ses fournisseurs ont mis en place des plans de continuité des services; vi. Une description du processus utilisé pour mettre à l'essai le plan de continuité des services; vii. Les mesures que l'entrepreneur prendra si un de ses principaux fournisseurs met fin à ses activités; viii. Les mesures que l'entrepreneur prendra si un des fabricants d'équipement d'origine n'est plus considéré comme un fabricant de confiance ou un fabricant d'équipement d'origine par le BT.	

SR-62	Intervention en cas d'incident	L'entrepreneur devrait fournir une version définitive du plan de continuité des services conformément à l'énoncé des travaux suivant la réception des commentaires du BT sur la version préliminaire.	
SR-63	Intervention en cas d'incident	Après avoir reçu l'acceptation du plan de continuité des services par le BT, l'entrepreneur devrait mettre en œuvre le plan (ensemble de processus, de procédures, de rôles et de responsabilités, etc.) et toute mise à jour annuelle ultérieure conformément à l'énoncé des travaux.	
SR-64	Intervention en cas d'incident	L'entrepreneur devrait fournir au BT, conformément à l'énoncé des travaux, des éléments de preuve (p. ex., résultats d'essai, évaluations et vérifications), datant des 12 derniers mois, pour démontrer que le plan de continuité des services a été convenablement mis en œuvre, qu'il fonctionne comme prévu, qu'il produit les résultats escomptés et qu'il satisfait aux exigences du BT en matière de continuité des services.	
SR-65	Intervention en cas d'incident	Si l'entrepreneur détermine qu'il faudra plus de temps que prévu dans l'énoncé des travaux pour présenter la preuve demandée pour le plan de continuité des services, il devrait en aviser le BT, par écrit et avec justification à l'appui, conformément aux dispositions de l'énoncé des travaux après la demande de preuve initiale et solliciter une prolongation. La décision d'accorder ou non une prolongation sera laissée à la discrétion du BT.	
SR-66	Intervention en cas d'incident	L'entrepreneur devrait répondre aux alertes de sécurité, aux avis et aux directives d'organisations externes désignées, approuvées par le BT, de manière continue, notamment comme suit : a) Surveiller constamment les alertes, les avis et les directives de sécurité; b) Créer les alertes, les avis et les directives de sécurité internes jugés nécessaires ou demandés par le bt; c) Diffuser les alertes, les avis et les directives de sécurité auprès des opérateurs ayant des responsabilités en matière de sécurité; d) Mettre en œuvre les directives de sécurité conformément aux délais établis, ou aviser le BT du niveau de non-conformité.	II-1, II-4, II-6, II-8, SI-5, SI-5(1)
SR-67	Intervention en cas d'incident	En plus des sources de renseignement sur les menaces et les incidents cybernétiques analysées dans le cadre de ses opérations de routine, l'entrepreneur devrait surveiller les publications sur le même sujet provenant des sources désignées par le Canada, comme le Centre canadien de réponse aux incidents cybernétiques	II-1, II-4, II-8,

		(http://www.sécuritépublique.gc.ca/prg/em/ccirc/anre-fra.aspx).	
SR-68	Intervention en cas d'incident	L'entrepreneur devrait mettre sur pied un Centre des opérations de sécurité avant la fin de la phase de préparation opérationnelle, et fournir l'infrastructure et les ressources nécessaires à la surveillance et à la résolution centralisées (24 heures sur 24, 7 jours sur 7) des incidents de sécurité liés au SGDSL.	II-1
SR-69	Intervention en cas d'incident	Le Centre des opérations de sécurité devrait : a) Coordonner l'intervention en cas d'incident de sécurité en étroite collaboration avec le BT; b) Offrir une ligne téléphonique unique et réservée, accessible en tout temps et dans la langue officielle du Canada (français ou anglais) demandée par l'appelant; c) Agir comme point de contact pour les communications avec les représentants du BT au sujet des incidents de sécurité; d) Ne pas perturber l'exploitation du SGDSL en cas de panne du Centre des opérations de sécurité (COS) de l'entrepreneur; e) Aviser le BT dans un délai de 15 minutes en cas de panne et fournir le nom de la personne-ressource avec qui le BT peut communiquer pendant la panne.	II-1, II-4, II-5, II-6, II-8
SR-70	Intervention en cas d'incident	Le Centre des opérations de sécurité devrait travailler avec le Centre de protection de l'information de SPC dans le cadre des activités suivantes : a) Intégration des processus; b) Surveillance; c) Traitement des incidents de sécurité et intervention en cas d'incident de sécurité; d) Vérification; e) Confinement, éradication et reprise en cas d'incident de sécurité, ce qui comprend : i. La capacité à dépêcher l'équipe de reprise après incident de sécurité de la ti sur le site de l'entrepreneur; ii. Le fait de permettre au BT d'assurer l'orientation et la coordination sur place.	II-1
SR-71	Intervention en cas d'incident	L'entrepreneur devrait automatiquement transmettre par courriel sécurisé les renseignements sur les dossiers d'incident aux destinataires d'une liste de diffusion prédéfinie pour chaque incident lié au BT, selon les spécifications suivantes fournies par ce dernier : a) Renseignements provenant du dossier d'incident;	II-1, II-2, II-4, II-5, II-6, II-8

		b) Fréquence des mises à jour; c) Listes de distribution; d) Critères de sélection des incidents (gravité, priorité, contenu du dossier d'incident).	
SR-72	Intervention en cas d'incident	L'entrepreneur devrait continuer d'envoyer automatiquement un courriel sécurisé lorsque le dossier d'incident est mis à jour, et ce, jusqu'à ce que le dossier d'incident soit clos ou que le BT annule la déclaration automatique des mises à jour.	II-1, II-2, II-4, II-5, II-6, II-8
SR-73	Intervention en cas d'incident	L'entrepreneur devrait mettre en œuvre des mesures d'atténuation (p. ex., blocage au moyen de pare-feu, signatures personnalisées des services de détection et de prévention d'intrusion, suppression des logiciels malveillants) afin de maîtriser un incident de sécurité, d'assurer une protection contre les cybermenaces et d'éliminer les vulnérabilités, à la demande des représentants autorisés du BT, conformément au niveau de priorité du Canada.	II-1, II-2, II-6
SR-74	Intervention en cas d'incident	L'entrepreneur devrait présenter un rapport rétrospectif sur l'incident de sécurité au BT dans les 72 heures suivant la demande de ce dernier, qui comprend entre autres ce qui suit : a) Le numéro de l'incident de sécurité; b) La date d'ouverture de l'incident de sécurité; c) La date de fermeture de l'incident de sécurité; d) Une description de l'incident de sécurité; e) La portée de l'incident de sécurité; f) La séquence et la chronologie des événements; g) Les mesures prises par l'entrepreneur; h) Les leçons retenues; i) Les limites ou problèmes liés à la solution du sgdsl; j) Les recommandations en vue d'améliorer la solution du SGDSL.	II-1, II-2, II-4, II-5, II-6, II-8
SR-75	Intervention en cas d'incident	L'entrepreneur devrait surveiller continuellement les événements dans l'infrastructure de la solution du SGDSL pour pouvoir faire ce qui suit : a) Détecter les attaques, les incidents et les événements anormaux dans la solution du SGDSL et l'infrastructure connexe; b) Détecter l'accès non autorisé aux données et aux composantes d'infrastructure de la solution du SGDSL; c) Assurer une intervention, un contrôle et une reprise des activités à la suite de menaces et d'attaques contre la solution du SGDSL.	II-1, II-2, II-4, II-5, II-6, II-8

SR-76	Intervention en cas d'incident	L'entrepreneur devrait donner de la formation aux opérateurs de l'infrastructure du SGDSL au sujet de leurs rôles et responsabilités en matière d'intervention en cas d'incident, et donner une formation d'appoint tous les ans.	II-2
SR-77	Intervention en cas d'incident	L'entrepreneur devrait mettre à l'essai le processus d'intervention en cas d'incident de la solution du SGDSL conformément à l'énoncé des besoins, au moyen de scripts complets, afin de vérifier l'efficacité du processus. Cela comprend ce qui suit : a) Consignation des résultats des essais; b) Examen des résultats des essais avec le bt; c) Mise en œuvre de mesures correctives selon les directives du bt, et dans le délai convenu avec ce dernier.	II-3
SR-78	Intervention en cas d'incident	L'entrepreneur devrait s'assurer que la posture de sécurité de la solution du SGDSL est maintenue en assurant de façon constante : a) La surveillance des menaces et des vulnérabilités; b) La surveillance des activités malveillantes et des accès non autorisés; c) L'adoption, s'il y a lieu, de contre-mesures proactives, y compris des mesures préventives et réactives pour atténuer les menaces.	II-4
SR-79	Intervention en cas d'incident	Le COS devrait : a) Accepter les courriels que les représentants autorisés du BT envoient à la boîte de réception fournie par l'entrepreneur et fournir automatiquement un accusé de réception; b) Accuser réception des courriels provenant d'adresses électroniques du SGDSL autorisées par le BT dans les 15 minutes suivant leur réception, et ce, en tout temps; c) Authentifier l'identité du demandeur au moyen d'un processus approuvé par le BT.	II-4
SR-80	Intervention en cas d'incident	L'entrepreneur devrait créer un ou plusieurs dossiers d'incident pour chaque incident relevé par l'entrepreneur ou signalé par le BT.	II-4
SR-81	Intervention en cas d'incident	L'entrepreneur devrait séparer physiquement ou logiquement l'information sur les incidents de sécurité de l'information sur tous les autres types d'incident. Tout renseignement sur les enquêtes liées à la sécurité généré dans le cadre du dossier devrait être enregistré dans le stockage dédié du BT.	II-4
SR-82	Intervention en cas d'incident	Lorsque l'entrepreneur détecte un incident ou que le BT en signale un, l'entrepreneur devrait ouvrir un dossier d'incident dans un délai de cinq minutes.	II-4

SR-83	Intervention en cas d'incident	L'entrepreneur devrait passer en revue les leçons apprises des activités de traitement des incidents et mettre en œuvre les mesures correctives qui s'ensuivent dans les procédures d'intervention en cas d'incident, ainsi que dans la formation, les essais et les exercices.	II-4
SR-84	Intervention en cas d'incident	Les dossiers d'incident de sécurité devraient inclure les renseignements supplémentaires suivants : a) Type et description de l'attaque ou de l'événement; b) La réussite apparente de l'attaque, et les répercussions; c) La portée de l'attaque; d) Le nombre estimatif de systèmes et de composantes de systèmes touchés; e) La liste des systèmes et des composantes touchées, par organisation; f) La source ou l'origine présumée de l'attaque, de l'incident ou de l'événement; g) La date et l'heure de l'attaque, de l'incident ou de l'événement; h) Le secteur ou le degré de préjudice estimatif; i) Le niveau d'incidence approximatif; j) La durée de l'attaque, de l'incident ou de l'événement; k) Les mesures prises; l) La situation relative aux mesures d'atténuation; m) Les journaux ou les données probantes applicables.	II-5
SR-85	Intervention en cas d'incident	L'entrepreneur devrait déclarer en tant qu'incident toutes les violations suspectes à la protection des renseignements personnels et à la sécurité relatives au SGDSL.	II-6
SR-86	Intervention en cas d'incident	L'entrepreneur devrait fournir tous les éléments de preuve associés à un incident de sécurité dans le format de fichier commercial et le délai précisés par le BT, y compris ce qui suit : a) Les registres et les dossiers de vérification selon les critères fournis par le BT; b) Des renseignements ou des données supplémentaires, selon les directives du BT.	II-6
SR-87	Intervention en cas d'incident	Lorsque l'entrepreneur détecte un incident ou que le BT en signale un, l'entrepreneur devrait ouvrir un dossier d'incident dans un délai de cinq minutes.	II-6
SR-88	Intervention en cas d'incident	L'entrepreneur devrait mettre à jour l'incident dans les cinq minutes suivant la modification de l'état d'un incident de grande priorité et dans les quinze minutes	II-6

		suivant la modification de l'état de tout autre type d'incident.	
SR-89	Intervention en cas d'incident	Les dossiers d'incident de l'entrepreneur devraient comprendre notamment les champs d'information suivants, qui devrait être tenus à jour : a) Le numéro de dossier attribué par l'entrepreneur; b) La description de l'incident; c) Les coordonnées du créateur du dossier (nom, numéro de téléphone et identificateur de la solution du SGDSL); d) La langue du créateur du dossier d'incident; e) Les dossiers d'incident connexes; f) La date et l'heure d'ouverture du dossier d'incident; g) La date et l'heure de fermeture du dossier d'incident; h) Le type du dossier d'incident (p. Ex., production, essai de fonctionnalité, essai de rendement, sécurité), selon les directives du BT; i) La gravité de l'incident; j) Les répercussions de l'incident; k) L'ordre de priorité du dossier d'incident; l) L'état du dossier d'incident (ouvert, fermé, en cours, suspendu, annulé, etc.); m) Les recours hiérarchiques relatifs au dossier d'incident; n) Le numéro de dossier attribué par le BT; o) Les fonctions de service touchées; p) Les points de prestation de service touchés; q) La personne-ressource de l'entrepreneur (nom, numéro de téléphone et identificateur de la solution du SGDSL); r) L'identifiant des partenaires (s'il y a lieu); s) Les interactions avec des tiers; t) Le journal des activités; u) La cause fondamentale de l'incident (si possible); v) Le temps estimatif requis pour résoudre l'incident (mis à jour toutes les 15 minutes); w) La description de la résolution; x) La durée de l'interruption (dossiers fermés seulement).	II-6
SR-90	Intervention en cas d'incident	Lorsque l'entrepreneur détecte un incident ou que le BT en signale un, l'entrepreneur devrait ouvrir un dossier d'incident dans un délai de cinq minutes.	II-6

SR-91	Intervention en cas d'incident	L'entrepreneur devrait mettre à jour l'incident dans les cinq minutes suivant la modification de l'état d'un incident de grande priorité et dans les quinze minutes suivant la modification de l'état de tout autre type d'incident.	II-6
SR-92	Intervention en cas d'incident	L'entrepreneur devrait, en tout temps, aviser le BT, par téléphone et à l'aide de la solution du SGDSL, selon l'ordre de priorité établi par le BT, de tout incident de sécurité réel ou suspect, notamment : a) Les attaques de rançongiciels; b) Les attaques par déni de service; c) Les logiciels malveillants; d) L'ingénierie sociale; e) L'intrusion ou l'accès non autorisé; f) La divulgation de renseignements confidentiels; g) Toute autre atteinte à la sécurité ou cybermenace ciblant le Canada.	II-6
SR-93	Intervention en cas d'incident	L'entrepreneur devrait divulguer au BT tous les renseignements et données qu'il possède relativement à la solution du SGDSL ou qui se rapportent à un incident de sécurité.	II-6
SR-94	Intervention en cas d'incident	L'entrepreneur devrait fournir un portail sécurisé de gestion de la sécurité afin de permettre au B de consulter tout renseignement relatif à la sécurité au sein de la solution du SGDSL. Cela comprend ce qui suit, entre autres : a) Des rapports d'incident de sécurité, des rapports rétrospectifs, des rapports spéciaux et les éléments de preuve afférents; b) Des dossiers d'incident de sécurité; c) Des rapports sur les activités des utilisateurs; d) Des rapports sur les activités des opérateurs; e) Des rapports sur les accès; f) Les rapports de vérification de la configuration; g) Les rapports sur les changements de la configuration; h) Des rapports de surveillance de l'intégrité des dossiers; i) Des rapports d'inventaire; j) Des rapports sur les vulnérabilités; k) Les rapports sur les changements de la configuration; l) Les demandes de changement d'urgence et les demandes de changement; m) Les correctifs et les correctifs de sécurité installés;	II-6

		n) Des renseignements sur le blocage ou le filtrage d'utilisateurs du sgdsl, le cas échéant, et la durée du blocage ou du filtrage; o) D'autres documents justificatifs (p. ex., liste blanche, liste noire).	
SR-95	Intervention en cas d'incident	L'entrepreneur devrait déclarer en tant qu'incident toutes les violations suspectes à la protection des renseignements personnels et à la sécurité relatives à la solution du SGDSL.	II-6
SR-96	Intervention en cas d'incident	Les réunions sur les incidents de sécurité ou les questions de sécurité déterminés par le BT devrait être tenues en personne dans la région de la capitale nationale durant les heures normales d'ouverture (de 8 h à 17 h, heure de l'Est), du lundi au vendredi et durant les heures de travail en dehors de cette période, selon ce dont conviennent l'entrepreneur et le BT.	II-7(2)
SR-97	Intervention en cas d'incident	L'entrepreneur devrait être disponible pour participer à une séance d'information sur les incidents de sécurité donnée par le Canada.	II-7(2)
SR-98	Intervention en cas d'incident	L'entrepreneur devrait avoir des procédures judiciaires et des mesures de protection en vigueur concernant ce qui suit : a) Gestion d'une chaîne de possession de l'information relative à la vérification; b) Collecte, conservation et présentation de preuves de l'intégrité des données.	II-8
SR-99	Intervention en cas d'incident	L'entrepreneur devrait élaborer un plan d'intervention en cas d'incident qui comprend ce qui suit : a) La façon dont l'entrepreneur compte détecter, signaler et acheminer les incidents de sécurité; b) Une feuille de route pour la mise en œuvre de la capacité d'intervention en cas d'incident de sécurité, y compris la préparation, la détection, l'analyse, le contrôle et la récupération; c) Une description de la structure et de l'organisation de la capacité d'intervention en cas d'incident de sécurité; d) Une approche d'ensemble concernant la façon dont la capacité d'intervention en cas d'incident de sécurité s'intègre dans l'organisation générale de l'entrepreneur; e) La définition des incidents de sécurité à signaler; f) La définition des mesures servant à évaluer la capacité d'intervention en cas d'incident de sécurité; g) La définition des ressources et du soutien de la direction nécessaires pour maintenir et faire	II-8

		évoluer la capacité d'intervention en cas d'incident de sécurité.	
SR-100	Maintenance du système	L'entrepreneur devrait procéder à la maintenance dirigée, comme suit : a) En planifiant, en exécutant et en consignant la maintenance et les réparations des composantes de la solution du SGDSL conformément aux spécifications du fabricant ou de l'entrepreneur, et en examinant les dossiers de maintenance; b) En supervisant toutes les activités de maintenance, qu'elles soient exécutées sur les lieux ou à distance et que l'équipement soit entretenu sur les lieux ou dans un autre emplacement; c) En demandant l'autorisation explicite d'un représentant désigné pour retirer certaines composantes de l'infrastructure de la solution du SGDSL du centre de données de l'entrepreneur aux fins de maintenance ou de réparations hors site; d) En nettoyant l'équipement informatique afin d'effacer toutes les données des supports d'information qui y sont associés avant de le sortir des installations de l'entrepreneur à des fins de maintenance ou de réparation à l'extérieur des lieux; e) En vérifiant toutes les exigences relatives à la sécurité pertinentes pour s'assurer que les contrôles fonctionnent toujours correctement à la suite des activités de maintenance ou de réparation.	MA-2, MA-2(1), MA-2(2)
SR-101	Maintenance du système	L'entrepreneur devrait approuver, contrôler, surveiller et entretenir de façon continue le matériel et les logiciels utilisés pour la maintenance de l'infrastructure du SGDSL, en particulier pour ce qui est du diagnostic et des réparations (p. ex., outils matériels ou logiciels introduits pour effectuer une activité de maintenance en particulier).	MA-3
SR-102	Maintenance du système	L'entrepreneur devrait : a) Inspecter les outils de maintenance apportés dans une installation par le personnel de maintenance pour s'assurer qu'aucune modification inappropriée ou non autorisée n'a été apportée; b) Vérifier que tous les supports d'information contenant des programmes de diagnostic et d'essai ne comportent aucun programme	MA-3(2), MA-3(3), MA-3(4)

		malveillant avant d'autoriser leur utilisation dans les composantes de l'infrastructure du SGDSL; c) Empêcher l'enlèvement non autorisé d'équipement de maintenance qui contient des données de la solution du SGDSL, au moyen des mesures suivantes : i. S'assurer que l'équipement ne contient aucun renseignement du SGDSL; ii. Nettoyer ou détruire l'équipement de maintenance; iii. Conserver l'équipement dans les installations de la solution du SGDSL ou obtenir une exemption précise d'une autorité contractante désignée de la solution du SGDSL concernant l'enlèvement de l'équipement des installations; d) Ne permettre l'utilisation des outils de maintenance que par le personnel autorisé.	
SR-103	Maintenance du système	L'entrepreneur devrait autoriser, surveiller et contrôler les activités de maintenance et de diagnostic au sein de l'infrastructure du SGDSL, comme suit : a) Permettre l'utilisation des outils de maintenance et de diagnostic approuvés par le BT (à discuter); b) Utiliser des techniques fortes d'identification et d'authentification étroitement liées à l'utilisateur pour l'ouverture de sessions de maintenance et de diagnostic, et séparer ces sessions des autres sessions du réseau dans l'infrastructure de la solution du SGDSL par l'un des moyens suivants : i. En utilisant des voies de communication physiques ou logiques distinctes; ou ii. En utilisant des voies de communication logiques distinctes établies au moyen de modules et d'algorithmes cryptographiques approuvés par le CSEC; c) Enregistrer les sessions de maintenance et de diagnostic; d) Faire examiner par des employés désignés les sessions de maintenance et de diagnostic enregistrées.	MA-4, MA-4(1)

SR-104	Maintenance du système	L'entrepreneur devrait définir un processus d'autorisation du personnel de maintenance, y compris ce qui suit : a) La tenue à jour d'une liste des organisations et du personnel responsables de la maintenance; b) La vérification que le personnel qui procède à la maintenance de la solution du sgdsl du ct dispose des autorisations d'accès nécessaires; c) La désignation de membres du personnel disposant des autorisations d'accès requises pour superviser la maintenance lorsque le personnel de maintenance n'a pas ces autorisations.	MA-5
SR-105	Protection des supports	L'entrepreneur devrait présenter au BT les procédures opérationnelles de sécurité qui comprennent les exigences en matière de protection des supports précisées dans le présent énoncé des travaux.	PS-1
SR-106	Protection des supports	L'entrepreneur devrait faire ce qui suit : a) Limiter aux opérateurs autorisés l'accès aux supports de TI (numériques et non numériques) qui contiennent des données de la solution du SGDSL; b) Utiliser des mécanismes pour vérifier les tentatives d'accès et les accès accordés.	PS-2, PS-2(1)
SR-107	Protection des supports	Conformément aux dispositions du contrat, l'entrepreneur devrait marquer les supports de TI amovibles contenant de l'information appartenant au Canada en indiquant les restrictions en matière de diffusion et de manipulation et les indications de sécurité applicables (le cas échéant).	PS-3
SR-108	Protection des supports	L'entrepreneur devrait faire ce qui suit : a) Contrôler physiquement et logiquement les supports de TI contenant des données de la solution du SGDSL conformément au document G1-001 de la GRC intitulé Guide d'équipement de sécurité; b) Protéger les supports qui contiennent des données de la solution du SGDSL jusqu'à la destruction ou le nettoyage du support au moyen d'équipement de techniques et de procédures approuvés (conformément à l'ITGS-06, Effacement et déclassification des supports d'information électroniques, du CSTC).	PS-4
SR-109	Protection des supports	L'entrepreneur devrait utiliser des mécanismes de chiffrement pour protéger l'information stockée de la solution du SGDSL qui sont approuvés par le BT et conformes aux directives du CSTC (ITSP.40.111).	PS-4(1)

SR-110	Protection des supports	L'entrepreneur devrait nettoyer et vérifier les supports de TI contenant des données de la solution du SGDSL (numériques et non numériques), avant leur élimination, leur retrait du contrôle de l'organisation ou leur retrait en vue d'une réutilisation.	PS-6 PS-6(1)
SR-111	Protection des supports	L'entrepreneur doit assurer le suivi et le contrôle des activités de nettoyage des supports et vérifier celles-ci en faisant ce qui suit : a) Mener les activités de nettoyage des supports conformément aux exigences applicables aux renseignements Protégé B énoncées dans le document ITSG-06 (http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-fra.html); b) Consigner les activités de nettoyage des supports; c) Au moins une fois par année, mettre à l'essai l'équipement et la procédure de nettoyage afin d'en vérifier le rendement; d) Nettoyer les appareils de stockage usagés qui ont été réaffectés avant de les raccorder à l'infrastructure du SGDSL du BT.	PS-6(2), PS-6(3), PS-6(4), PS-6(5), PS-6(6)
SR-112	Protection physique et environnemental e	L'entrepreneur devrait présenter au BT les procédures opérationnelles de sécurité qui définissent les exigences en matière de protection physique et environnementale précisées dans le présent énoncé des travaux.	PPE-1
SR-113	Protection physique et environnemental e	L'entrepreneur devrait mettre en œuvre un système de gestion de l'accès physique fondé sur les rôles pour les installations de l'infrastructure de SGDS qui comprend ce qui suit : a) Tenue d'une liste du personnel autorisé à accéder aux installations; b) Émission de justificatifs d'autorisation d'accès aux installations; c) Examen et approbation de la liste d'accès et des justificatifs d'autorisation à tout moment et au moins tous les mois, en retirant de la liste d'accès le nom des membres du personnel qui n'ont plus besoin d'accéder aux installations; d) Autorisation de l'accès physique aux installations, par point d'accès, en fonction du rôle de la personne; e) Modification de l'attribution lorsque l'utilisateur assume un nouveau rôle; f) Séparation des tâches de manière à ce que l'autorisation d'accéder aux installations soit accordée par une autre personne que celle qui	PPE-2, PPE-2(1), PPE-2(2), PPE-2(3), Exigence spécifique du document ITSG-33 du CSTC : PPE-2(100), SP-5

		autorise l'accès à l'infrastructure de la solution du sgdsl; g) Attribution au personnel de l'autorisation d'accéder aux installations en fonction de leur besoin de savoir et leur besoin d'accès; h) Autorisations d'accès physique aux installations de la solution du SGDSL accordées par l'entrepreneur distinctes de l'autorisation d'accès physique aux locaux où sont situées ces installations; i) communication avec la GRC si un accès en cas d'urgence est requis.	
SR-114	Protection physique et environnemental e	L'entrepreneur devrait déposer un plan de sécurité de l'immeuble à l'examen du BT, lequel plan comprend notamment : a) Le plan de sécurité physique pour les points de contrôle d'accès; b) Les zones de sécurité physique; c) La surveillance des points d'accès physique; d) L'application par l'entrepreneur des autorisations d'accès physique pour tous les points d'accès physique (y compris les points d'entrée et de sortie désignés) aux installations où est située l'infrastructure (à l'exception des zones des installations officiellement accessibles au public); i. Vérifier les autorisations d'accès individuelles avant d'accorder l'accès aux installations; ii. Contrôler l'accès aux installations où est située l'infrastructure au moyen de dispositifs d'accès physique ou de gardiens; iii. Contrôler l'accès aux zones officiellement accessibles au public en fonction de l'évaluation du risque de l'entrepreneur; iv. Garder les clés, les combinaisons et les autres dispositifs de contrôle de l'accès physique en lieu sûr; v. Répertorier les dispositifs d'accès physique au moins tous les ans; vi. Changer les combinaisons et les clés dès qu'une clé est perdue, qu'une combinaison est compromise ou que des personnes sont mutées ou congédiées.	PPE-3, PPE-3(1), PPE-3(2), PPE-3(3), PPE-3(4), PPE-3(5); PPE-3(6); PPE-4, PPE-5

SR-115	Protection physique et environnemental e	L'entrepreneur devrait surveiller l'accès physique aux installations de l'infrastructure de SGDSL comme suit : a) Surveillance en temps réel des alarmes d'intrusion physique et de l'équipement de surveillance; b) Enregistrement de tous les événements d'accès physique; c) Examen des registres d'accès physique au moins une fois par mois; d) Présentation des registres tous les mois et à la demande du bt; e) Création d'un incident de sécurité à la découverte d'une activité anormale.	PPE-6, PPE-6(1), PPE-6(3)
SR-116	Protection physique et environnemental e	L'entrepreneur devrait gérer l'accès physique aux installations de l'infrastructure de SGDSL comme suit : a) En procédant à l'authentification des visiteurs avant d'accorder, avec l'approbation du BT, les autorisations d'accès aux installations où est située l'infrastructure; b) En authentifiant les visiteurs au moyen de deux formes d'identification avant d'accorder un accès aux installations du SGDSL; c) En accompagnant les visiteurs et en surveillant les activités des visiteurs dans les installations de la solution du SGDSL en tout temps.	PPE-7, PPE-7(1), PPE-7(2)
SR-117	Protection physique et environnemental e	L'entrepreneur devrait autoriser, surveiller et contrôler toutes les composantes qui entrent dans les installations d'infrastructure de la solution du SGDSL et qui en sortent, et tenir des dossiers sur ces composantes et ces activités. Les dossiers devrait être fournis chaque mois et à la demande du gouvernement du Canada.	PPE-16
SR-118	Protection physique et environnemental e	L'entrepreneur devrait faire ce qui suit : a) Mettre en œuvre dans des sites de remplacement des contrôles de gestion, des activités et de sécurité technique permettant d'atteindre les mêmes objectifs que les contrôles mis en place dans les installations de la solution du SGDSL; b) Faire approuver par la Direction de la sécurité industrielle canadienne ou la Direction de la sécurité industrielle internationale le site de remplacement en même temps que les sites principaux.	PPE-17, SP-1
SR-119	Sécurité du personnel	À la cessation d'emploi d'une personne associée à la solution du SGDS, l'entrepreneur devrait faire ce qui suit :	SP-4

		a) Mettre fin à l'accès physique de l'employé aux installations d'infrastructure du SGDSL; b) Mettre fin à son accès à l'infrastructure du SGDSL, y compris à son accès à distance; c) Récupérer tous les biens liés à la sécurité (p ex., la carte d'identité de l'employé, un jeton d'authentification physique).	
SR-120	Sécurité du personnel	L'entrepreneur devrait gérer les comptes des utilisateurs de l'infrastructure de la solution du SGDSL de la manière suivante : a) Création de comptes d'utilisateur assortis de profils d'accès en fonction de rôles qui déterminent les privilèges; b) Suivi et surveillance de l'attribution de rôles aux utilisateurs; c) Modification de l'attribution du rôle lorsque l'utilisateur assume un nouveau rôle.	SP-5
SR-121	Sécurité du personnel	L'entrepreneur devrait préparer des ententes concernant l'accès à l'infrastructure ou aux données de la solution du SGDSL. L'entrepreneur devrait s'assurer que les opérateurs qui ont besoin d'accéder aux systèmes d'information et à l'information de l'organisation : a) Signent les ententes d'accès appropriées avant d'obtenir l'accès; b) Signent les nouvelles ententes d'accès lorsque celles-ci sont mises à jour. L'entrepreneur devrait examiner et mettre à jour les ententes concernant l'accès à l'infrastructure du SGDSL tous les deux ans.	SP-6
SR-122	Sécurité du personnel	L'entrepreneur devrait faire ce qui suit : a) S'assurer que les opérateurs signent une entente concernant l'accès (avant d'obtenir l'accès à l'infrastructure ou aux données de la solution du SGDSL) qui présente le processus de sanction officiel en cas de non-respect des modalités de ladite entente; b) Donner aux opérateurs de l'infrastructure de la solution du SGDSL une formation sur leurs responsabilités en matière de protection des renseignements personnels et de la confidentialité des données du SGDSL conformément aux modalités du contrat de la solution du SGDSL et aux sanctions prévues en cas de non-respect. L'entrepreneur devrait donner une formation d'appoint deux fois par année.	SP-8

SR-123	Évaluation des risques	L'entrepreneur devrait permettre au BT, ou à ses représentants, d'effectuer une évaluation de la vulnérabilité de la solution du SGDSL, comme énoncé dans un énoncé des travaux associé à une demande du BT, qui comprend ce qui suit : a) Accès physique aux installations de la solution du SGDSL, c.-à-d. Les installations de l'entrepreneur où est située l'infrastructure (p. Ex, matériel et logiciels) du SGDSL; b) L'accès au réseau de l'infrastructure de la solution du SGDSL afin de permettre un balayage authentifié et non authentifié des composantes du réseau et des appareils de sécurité, à l'aide de l'équipement exploité par le BT et des outils précisés par ce dernier; c) Le soutien, par au moins une ressource technique qui connaît les aspects techniques de la solution du SGDSL, durant la partie de l'évaluation de la vulnérabilité effectuée sur place (matériel, logiciel, composantes du réseau, appareils de sécurité, configuration); d) Le BT limitera son évaluation à des activités de détection et d'analyse de l'infrastructure de la solution du SGDSL et n'entreprendra pas d'activités perturbatrices ou destructives.	ER-5
SR-124	Acquisition de systèmes et de services	À compter de la date de signalement de vulnérabilités, l'entrepreneur devrait, à tout le moins : a) Atténuer toutes les vulnérabilités à risque élevé dans les 10 jours; b) Atténuer toutes les vulnérabilités à risque modéré dans les 30 jours. Le BT et l'entrepreneur devrait déterminer la cote de risque des vulnérabilités et convenir mutuellement de celle-ci. L'entrepreneur devrait faire ce qui suit : a) Incorporer les facteurs de sécurité de l'information lorsqu'il développe, personnalise ou modifie la solution du SGDSL; b) Définir et consigner les rôles et responsabilités associés à la sécurité de l'information tout au long du cycle de développement du système; c) Identifier les personnes auxquelles sont attribués des rôles et des responsabilités associés à la sécurité du système d'information; d) Intégrer les processus organisationnels de gestion des risques liés à la sécurité de	ASS-3

		l'information aux activités du cycle de développement du système.	
SR-125	Acquisition de systèmes et de services	L'entrepreneur devrait maintenir l'état d'autorisation de sécurité de la solution du SGDSL au moyen d'une surveillance soutenue et de vérifications annuelles des exigences en matière de sécurité mises en œuvre dans le cadre de la solution du SGDSL afin de déterminer si les mesures relatives à la sécurité du système d'information sont toujours efficaces au fil du temps, à la lumière des modifications apportées à la solution du SGDSL et à son environnement opérationnel.	ASS-3
SR-126	Acquisition de systèmes et de services	L'entrepreneur devrait fournir des preuves à l'appui des activités de maintien des autorisations dans les 30 jours suivant une demande du BT, à la suite de tous les changements apportés à l'infrastructure du SGDSL par l'entrepreneur.	ASS-3
SR-127	Acquisition de systèmes et de services	L'entrepreneur devrait, à la demande du BT et dans les 30 jours de celle-ci, mettre à jour les procédures opérationnelles de sécurité et démontrer leur mise en œuvre dans le cadre des activités de maintien des autorisations.	ASS-3
SR-128	Acquisition de systèmes et de services	L'entrepreneur doit restreindre l'emplacement des services de traitement de l'information, d'information/données et de systèmes d'information au Canada.	ASS-9(5)
SR-129	Protection du système et des communications	L'entrepreneur doit inclure, dans les procédures opérationnelles de sécurité, une politique et des procédures visant à faciliter la mise en œuvre et la tenue à jour, des exigences en matière de protection du système et des communications, qui sont précisées dans le présent énoncé des travaux et dans les normes applicables du gouvernement du Canada mentionnées dans le présent énoncé des travaux.	SC-1
SR-130	Protection du système et des communications	La solution du SGDSL devrait comprendre une fonction de protection contre les attaques par déni de service qui limite le nombre de connexions simultanées selon les directives du BT.	SC-5, SC-5(1), SC-5(2)
SR-131	Protection du système et des communications	a) La conception de la solution du SGDSL devrait respecter l'établissement des zones de sécurité dans un réseau conformément aux Conseils et directives en matière de sécurité des technologies de l'information (ITSG) 22 et 38. De plus. l'infrastructure du SGDSL devrait surveiller et contrôler les communications à la limite externe du système et aux principales limites internes du système conformément à l'ITSG-22 et à l'ITSG-38.	SC-7

		b) L'entrepreneur devrait surveiller et analyse le trafic réseau, en temps quasi réel, pour détecter les attaques et les signes de composantes compromises de l'infrastructure de la solution du SGDSL. c) L'entrepreneur devrait détecter les attaques, par exemple : i. Les attaques de rançongiciels; ii. Les attaques par déni de service; iii. Les logiciels malveillants; iv. L'ingénierie sociale; v. L'intrusion ou l'accès non autorisé; vi. La divulgation de renseignements confidentiels; vii. Toute autre atteinte à la sécurité ou cybermenace ciblant le Canada.	
SR-132	Protection du système et des communications	L'infrastructure du SGDSL devrait se connecter uniquement aux réseaux ou aux systèmes d'information externes indiqués par le Canada par l'intermédiaire d'interfaces gérées, également indiquées par le Canada, au moyen de dispositifs de protection des limites installés conformément aux documents ITSG-22 et ITSG-38.	SC-7(2)
SR-133	Protection du système et des communications	L'entrepreneur devrait gérer activement toutes les connexions réseau aux services externes associés à l'infrastructure de la solution du SGDSL, comme suit : a) Refus par défaut de tout trafic sur le réseau; b) Définition du trafic permis pour chaque connexion réseau (refus systématique et autorisation par exception); c) Coupure de la connexion réseau associée à une séance de communication à la fin de la séance ou après un nombre défini de minutes d'inactivité selon les directives du bt; d) Consignation de chaque exception à la politique sur le flux du trafic en indiquant la nature et la durée du besoin; e) Examen des exceptions à la politique sur le flux du trafic au moins une fois par année; f) Suppression des exceptions à la politique sur le flux du trafic qui ne sont plus justifiées par un besoin opérationnel explicite; g) Surveillance du trafic pour détecter des activités ou des conditions inhabituelles ou non autorisées; h) Au besoin, surveillance du trafic à certains points à l'intérieur du système (p. ex., sous-	SC-7(4), SC-7(5)

		réseaux, sous-systèmes) pour déceler des anomalies.	
SR-134	Protection du système et des communications	L'entrepreneur devrait empêcher que les appareils qu'il gère (p. ex., ordinateur portatif ou autre appareil utilisé à des fins administratives) qui sont connectés à la solution du SGDSL établissent des communications à l'extérieur de cette voie de communication (p. ex., accéder à Internet à partir d'une connexion distincte disponible).	SC-7(7)
SR-135	Protection du système et des communications	L'infrastructure de la solution du SGDSL devrait détecter les extrusions en temps quasi réel.	SC-7(9)
SR-136	Protection du système et des communications	L'entrepreneur devrait surveiller et analyser les composantes des hôtes (prévention et détection des intrusions en mode hôte) en temps quasi réel afin de détecter les attaques et les indications d'hôtes compromis.	SC-7(12)
SR-137	Protection du système et des communications	L'entrepreneur devrait physiquement ou logiquement séparer le trafic réseau IP : a) Des données du système par rapport aux données de gestion et aux données d'utilisateur de la solution du SGDSL ; b) Des données de gestion par rapport aux données d'utilisateurs du SGDSL.	SC-7(13)
SR-138	Protection du système et des communications	L'entrepreneur devrait configurer les mesures de protection des limites (p. ex., pare-feu) au mode au mode de sécurité (aucune transmission de trafic) dès qu'une défaillance survient.	SC-7(18)
SR-139	Protection du système et des communications	La conception de la solution du SGDSL doit : a) Permettre l'authentification mutuelle des connexions entre la solution du SGDSL et les autres domaines, selon les directives du BT et autoriser exclusivement l'échange d'information avec ces autres domaines en utilisant l'authentification mutuelle; b) Garantir que l'intégrité et la confidentialité des données du SGDSL, durant la transmission et en période d'arrêt, sont protégées à l'aide de solutions cryptographiques, sauf si elles sont protégées par d'autres mécanismes approuvés par le BT.	SC-8
SR-140	Protection du système et des communications	L'infrastructure de la solution du SGDSL doit protéger l'intégrité et la confidentialité des données du SGDSL durant la transmission et en période d'arrêt à l'aide des modules et des algorithmes cryptographiques approuvés par le CSTC, à moins qu'elles ne soient protégées autrement par d'autres mesures de protection physique approuvées par le BT.	SC-8(1)

SR-141	Protection du système et des communications	La conception du SGDSL doit : a) Permettre l'authentification mutuelle des connexions entre la solution du SGDSL et les autres domaines, selon les directives du BT et autoriser exclusivement l'échange de messages avec ces autres domaines en utilisant l'authentification mutuelle; b) Garantir que l'intégrité et la confidentialité des données du SGDSL, durant la transmission et en période d'arrêt, sont protégées à l'aide de solutions cryptographiques, sauf si elles sont protégées par d'autres mécanismes approuvés par le BT; c) Etre conforme aux zones de sécurité de réseau, conformément à l'itsg-22 et à l'itsg-38; d) Chiffrer les renseignements sur les incidents de sécurité selon les normes de chiffrement si les renseignements sont transmis en format électronique.	SC-9, SC-9(1), SC-9(2), SC-12(1), SC-12(2), SC-12(3), SC-12(4), SC-12(5), Exigence spécifique du document ITSG-33 du CSTC : SC-9(100)
SR-142	Protection du système et des communications	L'entrepreneur devrait s'assurer que la conception du SGDSL utilise des solutions de cryptographiques (p. ex., RPV, protocole TLS, modules logiciels, ICP et jetons d'authentification, s'il y a lieu) dans les conditions suivantes : a) Utilisation d'algorithmes cryptographiques, de tailles de clés cryptographiques ainsi que des cryptopériodes approuvés par le CSTC et validés dans le cadre du Programme de validation des algorithmes cryptographiques, et précisés dans le document ITSB-111 (https://www.cse-cst.gc.ca/fr/node/1428/html/25015); b) Mise en œuvre dans un module cryptographique validé dans le cadre du Programme de validation des modules cryptographiques à tout le moins au niveau 1 de la norme FIPS 140-2; c) Fonctionnement en mode FIPS.	SC-13, Exigence spécifique du document ITSG-33 du CSTC : SC-13(100), SC-13(101)
SR-143	Protection du système et des communications	L'entrepreneur ne devrait pas empêcher un utilisateur de chiffrer, de déchiffrer, de signer et de vérifier des fichiers en pièce jointe du SGDSL à l'aide de certificats approuvés par l'autorité contractante du gouvernement du Canada.	SC-17
SR-144	Protection du système et des communications	L'entrepreneur devrait utiliser uniquement le code mobile approuvé au préalable dans l'infrastructure de la solution du SGDSL et devrait donc refuser le téléchargement et l'exécution de tout autre code mobile.	SC-18, SC-18(1), SC-18(2), SC-18(3), SC-18(4)

SR-145	Protection du système et des communications	La ou les composantes de l'infrastructure de la solution du SGDSL qui fournissent collectivement un service de résolution du nom ou de l'adresse pour ***La solution SGDSL*** devrait effectuer une distinction des rôles internes et des rôles externes.	SC-22
SR-146	Protection du système et des communications	La solution du SGDSL devrait permettre l'authentification de tous les types de clients logiciels au moyen d'un justificatif de la solution du SGDSL.	SC-23
SR-147	Protection du système et des communications	L'infrastructure de la solution du SGDSL devrait protéger l'intégrité et la confidentialité des données du SGDSL durant la transmission et en période d'arrêt à l'aide des modules et des algorithmes cryptographiques approuvés par le CSTC, à moins qu'elles ne soient protégées autrement par d'autres mesures de protection physique approuvées par le BT.	SC-28
SR-148	Protection du système et des communications	L'entrepreneur peut, à sa discrétion, utiliser du matériel et des logiciels non spécialisés pour l'exploitation, l'administration et la gestion des données relatives à la solution du SGDSL. L'utilisation du matériel et de logiciels non réservés n'est autorisée que pour les données de gestion de la solution du SGDSL, selon les conditions suivantes : a) Ne pas traiter ou stocker des données d'utilisateurs du SGDSL ou y accéder; b) Ne pas traiter ou stocker des données du système du SGDSL ou y accéder; c) Ne pas traiter ou stocker les noms et aux mots de passe des comptes d'utilisateurs, ou y accéder; d) Séparer logiquement les données de gestion des autres données du client; e) Respecter les exigences relatives à l'infrastructure de la solution du SGDSL énoncées dans la présente liste d'exigences en matière de sécurité; f) Ne pas traiter ou stocker de renseignements protégés ou classifiés, ou y accéder, sans autorisation par écrit du BT; g) Ne pas traiter ou stocker l'information de conception de la solution du SGDSL, ou y accéder; h) Ne pas permettre le contrôle ou la modification de l'infrastructure de la solution du SGDSL du BT.	SC-32
SR-149	Protection du système et des communications	***La solution SGDSL*** devrait comprendre des contrôles spécialisés pour toute interconnexion réseau entre l'infrastructure spécialisée ou non spécialisée de la	SC-32

		solution du SGDSL, conformément à l'architecture de sécurité approuvée, qui comprend ce qui suit : a) La protection du périmètre, où l'entrepreneur devrait utiliser les pare-feu physiques actuels ou évalués précédemment validés à l'aide d'un schéma lié aux Critères communs reconnu, selon un profil de protection approuvé portant sur l'évaluation des pare-feu. L'entrepreneur devrait obtenir l'approbation du BT pour utiliser un autre pare-feu physique; b) L'intégration d'un équipement de détection des menaces fourni par le BT; c) L'intégration de solutions de prévention ou de détection des menaces fournies par l'entrepreneur; d) L'acheminement du trafic par l'intermédiaire de serveurs mandataires authentifiés; e) Le contrôle d'accès en fonction de rôles avec droit d'accès minimal.	
SR-150	Protection du système et des communications	L'entrepreneur devrait : a) Physiquement ou logiquement séparer les renseignements qui déterminent et décrivent les incidents de sécurité de tous les autres types d'incidents. Tout renseignement sur les enquêtes liées à la sécurité généré dans le cadre du dossier devrait être enregistré dans le stockage dédié du BT; b) Veiller à ce que tous les détails sur la configuration du réseau contenus dans les dossiers des biens et les systèmes de gestion des dossiers de configuration de l'infrastructure de la solution du SGDSL soient chiffrés; c) Séparer données de système sur le trafic réseau IP de la solution du SGDSL des autres données du SGDSL; d) Séparer logiquement le trafic IP sur le réseau entre les données sur la gestion du SGDSL et les données d'utilisateurs du SGDSL.	SC-32
SR-151	Protection du système et des communications	La catégorisation des données de la solution du SGDSL selon qu'il s'agit de données du système, des utilisateurs ou de gestion, sera à l'entière discrétion du BT et sera fondée sur une comparaison avec d'autres données similaires.	SC-32
SR-152	Intégrité du système et des renseignements	L'entrepreneur devrait présenter au BT des procédures opérationnelles de sécurité relatives à la solution du SGDSL qui définissent les rôles et les responsabilités opérationnels en vue de satisfaire aux exigences en	SI-1

		matière d'intégrité du système et des renseignements énoncées dans le présent énoncé des travaux.	
SR-153	Intégrité du système et des renseignements	L'entrepreneur devrait définir et exécuter les processus de gestion des correctifs pour les composantes d'infrastructure de la solution du SGDSL, notamment : a) L'utilisation de la version à jour des applications et des systèmes d'exploitation; b) Le fait de veiller à ce que les vulnérabilités soient évaluées et à ce que les correctifs de sécurité fournis par le fournisseur soient appliqués rapidement; c) L'établissement de l'ordre de priorité des correctifs critiques à l'aide d'une approche fondée sur le risque; d) La mise hors ligne et la remise en ligne des applications; e) L'harmonisation des niveaux de criticité des correctifs, selon les directives du BT; f) L'attribution d'une cote aux vulnérabilités qui s'appuie sur la version 3.0 du CVSS; g) L'utilisation d'une méthode de mise à l'essai et de vérification pour s'assurer que les correctifs sont mis en œuvre correctement; h) La définition de processus de gestion des correctifs pour les logiciels personnalisés utilisés dans la solution du SGDSL, y compris ce qui suit : i. La détection, le signalement et la correction des failles dans les logiciels personnalisés; ii. La mise à l'essai des mises à jour destinées à corriger les failles afin d'en déterminer l'efficacité et les éventuels effets sur les services liés à la solution du SGDSL avant de procéder à leur installation; iii. L'incorporation de la correction des failles dans le processus de gestion de la configuration pour la solution du SGDSL.	SI-2, SI-2(1), SI-2(2), SI-2(3), SI-2(4)
SR-154	Intégrité du système et des renseignements	L'entrepreneur devrait faire ce qui suit : a) Centraliser la gestion des mécanismes de protection contre les programmes malveillants; b) Mettre automatiquement à jour les mécanismes de protection contre les programmes ou les logiciels malveillants (y compris les définitions de signature) dans les	SI-3(1), SI-3(2), SI-3(3), SI-3(4), SI-3(5)

		six heures suivant le moment où ils sont rendus disponibles et à la demande du BT; c) Empêcher les utilisateurs non privilégiés de contourner les capacités de protection contre les programmes malveillants; d) Mettre à jour les mécanismes de protection contre les programmes malveillants uniquement à la demande d'un utilisateur privilégié; e) Empêcher les utilisateurs d'introduire des supports amovibles dans l'infrastructure de la solution du SGDSL.	
SR-155	Intégrité du système et des renseignements	L'infrastructure de la solution du SGDSL devrait générer des alertes en temps quasi réel (p. ex., au moyen de règles de corrélation) lorsqu'il y a des indications de compromission réelle ou possible.	SI-4(5)
SR-156	Intégrité du système et des renseignements	L'infrastructure du SGDSL devrait empêcher les utilisateurs non privilégiés de contourner les fonctions de détection et de prévention des intrusions.	SI-4(6)
SR-157	Intégrité du système et des renseignements	L'entrepreneur devrait mettre en œuvre une solution de vérification de l'intégrité gérée de façon centralisée visant à détecter les changements non autorisés à la configuration des composantes de l'infrastructure de la solution du SGDSL et des logiciels, notamment : a) La vérification de l'intégrité au moins tous les 30 jours; b) La génération automatique d'un dossier d'incident de sécurité à la découverte d'anomalies pendant la vérification de l'intégrité.	SI-7, SI-7(1), SI-7(2)

14.1.2 Contrôles de sécurité de l'industrie pour La solution SGDSL

Voici des exigences supplémentaires en matière de sécurité tirées du cadre Cloud Controls Matrix Version 3.0.1, du FedRAMP, des normes NIST 800-53 et 800-171, et de la norme ISO/IEC 27001 :

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
SR-158	Gestion du cycle de vie de l'information et de la sécurité des données Répertoire et flux de données	Les politiques et les procédures de la solution du SGDSL devrait être établies afin de répertorier, de consigner et de tenir à jour les flux de données pour ce qui est des données qui se trouvent (de façon permanente ou temporaire) dans les applications, l'infrastructure, le réseau et les systèmes du service. Plus particulièrement, l'entrepreneur devrait s'assurer que les données visées par des exigences	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		relatives à leur emplacement géographique ne sont pas migrées à l'extérieur des limites définies.	directives ministérielles
SR-159	Gestion du cycle de vie de l'information et de la sécurité des données Données non liées à la production	Les données de production de la solution du SGDSL ne devrait pas être reproduites ni utilisées dans des environnements de non-production.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-160	Chiffrement et gestion des clés Admissibilité	Les propriétaires des clés de l'infrastructure à clés publiques de la solution du SGDSL devrait être identifiables (lier les clés aux identités), et des politiques de gestion des clés doivent être établies.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-161	Chiffrement et gestion des clés Génération des clés	Des politiques et des procédures opérationnelles de la solution du SGDSL doivent être établies pour la gestion des clés cryptographiques dans le système cryptographique du service (p. ex., gestion du cycle de génération des clés jusqu'à la révocation et au remplacement, infrastructure à clés publiques, conception du protocole cryptographique et des algorithmes utilisés, contrôles d'accès en place pour la génération sécuritaire de clés, et échange et stockage, y compris répartition des clés utilisées pour les données ou les séances chiffrées). Sur demande, l'entrepreneur doit informer le BT des changements apportés au système cryptographique, en particulier si les données du SGDSL sont utilisées dans le cadre du service ou si le BT assume une responsabilité partagée pour ce qui est de la mise en œuvre du contrôle.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
SR-162	Chiffrement et gestion des clés Protection des données de nature délicate	Les politiques et les procédures opérationnelles de la solution du SGDSL doivent être établies, et les processus opérationnels à l'appui ainsi que les mesures techniques doivent être mis en œuvre en vue d'utiliser des protocoles de chiffrement pour la protection des données de nature délicate stockées (p. ex. serveurs de fichiers, base de données et postes de travail des utilisateurs finaux), des données en usage (mémoire) et des données en cours de transmission (p. ex. interfaces du système, réseaux publics, messagerie électronique), conformément aux obligations de conformité juridiques, législatives et réglementaires.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-163	Chiffrement et gestion des clés Stockage et accès	Le chiffrement de la plateforme de la solution du SGDSL et des données appropriées (conformément aux directives du CSTC énoncées dans le document ITSG-111) au moyen de formats ouverts et validés et d'algorithmes normalisés est requis. Les clés ne doivent pas être stockées dans le service hébergé géré e l'entrepreneur, mais plutôt être conservées par le BT ou par un entrepreneur de confiance chargé de gérer les clés, selon ce qui aura convenu mutuellement avec le BT. La gestion et l'utilisation des clés de la solution du SGDSL doivent représenter deux tâches distinctes.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-164	Gouvernance et gestion des risques Évaluations des risques axées sur les données	Les évaluations des risques de la solution du SGDSL associées aux exigences en matière de gouvernance des données doivent être réalisées aux intervalles prévus, comme il aura été mutuellement convenu avec le BT, et elles devraient tenir compte de ce qui suit : La connaissance de l'endroit où sont stockées et transmises les données de nature délicate dans les applications, les bases de données, les serveurs et l'infrastructure réseau; Le respect des périodes de conservation définies et des exigences relatives à l'élimination en fin de vie;	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		La classification des données et la protection de celles-ci contre l'utilisation, l'accès et la destruction non autorisés, ainsi que la perte et la falsification.	
SR-165	Gouvernance et gestion des risques Surveillance de la gestion	Les gestionnaires de l'entrepreneur sont chargés de se tenir au courant des politiques, des procédures et des normes en matière de sécurité qui se rapportent à leur zone de responsabilité, et de les respecter.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-166	Gouvernance et gestion des risques Programme de gestion	L'entrepreneur devrait avoir établi un programme de gestion de la sécurité de l'information, le consigner, le faire approuver et le mettre en œuvre. Ce programme devrait inclure des mesures de protection administratives, techniques et physiques pour protéger les biens et les données contre la perte, l'usage abusif, ainsi que l'accès, la divulgation, l'altération et la destruction non autorisés. Le programme de sécurité devrait notamment comprendre les domaines suivants, dans la mesure où ils sont liés aux caractéristiques de l'entreprise : Gestion des risques; Politique en matière de sécurité; Organisation de la sécurité de l'information; Gestion des biens; Sécurité liée aux ressources humaines; Sécurité physique et environnementale; Gestion opérationnelle et gestion de la communication; Contrôle de l'accès; Achat, développement et maintenance des systèmes d'information.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
SR-167	Gouvernance et gestion des risques Cadre de gestion des risques	Tous les risques associés à la solution du SGDSL devraient être atténués à un niveau acceptable. Des niveaux d'acceptation fondés sur des critères de risque devrait être établis et consignés conformément aux délais raisonnables de résolution et à l'approbation des intervenants.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-168	Partitionnement des appareils interréseau des zones	L'utilisation d'appareils virtuels dans l'interréseau des zones devrait être suffisamment séparée des serveurs virtuels dans toutes les zones d'infrastructure contenant des applications du SGDSL.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-169	Partition du stockage	Le stockage de la solution du SGDSL utilisé par l'hyperviseur pour gérer les images des appareils virtuels doit être physiquement et logiquement séparé lorsque l'infrastructure du SGDSL contient des applications de niveau Protégé B pouvant causer des préjudices MOYENS, tel que défini par le BT.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-170	Utilisation des caractéristiques de l'hyperviseur	Les machines virtuelles propres à l'architecture du SGDSL ne devraient pas utiliser de mécanisme d'échange machine-machine (p. ex., échange de fichiers), ces derniers mécanismes étant déjà mis en œuvre par l'hyperviseur.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-171	Certification de l'hyperviseur	L'entrepreneur doit utiliser les hyperviseurs couramment ou précédemment évalués afin de gérer toutes les zones, tel que défini dans les	Exigences adaptées en fonction des

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		directives des documents ITSG-22 (https://cse-cst.gc.ca/fr/node/268/html/15236) et ITSG-38 (https://cse-cst.gc.ca/fr/node/266/html/25034) [https://cse-cst.gc.ca/fr/group-groupe/schema-canadien-lie-aux-criteres-communs]), validés à l'aide d'un schéma lié aux Critères communs reconnus, selon un profil de protection approuvé portant sur l'évaluation des hyperviseurs pour la protection des machines virtuelles entre les zones, ou il doit obtenir l'approbation du BT pour utiliser des produits de remplacement.	pratiques exemplaires de l'industrie et des directives ministérielles
SR-172	GIJIA	La solution provisoire GIJIA de l'entrepreneur devrait supprimer tous les justificatifs d'identité du GC lorsqu'ils auront été entièrement transférés à la solution GIJA du GC.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-173	Sécurité de la virtualisation et de l'infrastructure Gestion des vulnérabilités	L'entrepreneur devrait s'assurer que les outils ou les services d'évaluation des vulnérabilités de sécurité sont adaptés aux technologies de virtualisation utilisées (p. ex. équipement d'alerte et d'enregistrement automatiques de virtualisation) dans la solution du SGDSL.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-174	Sécurité de la virtualisation et de l'infrastructure Environnements de production et de non-production	Les environnements de production et de non-production de la solution du SGDSL doivent être séparés afin de prévenir tout accès ou changement non autorisé aux ressources d'information. La séparation des environnements peut comprendre : des pare-feu à inspection dynamique, des sources d'authentification des domaines ou des partitions, et une séparation claire des tâches pour le personnel ayant accès à ces environnements dans le cadre de leurs fonctions, selon l'approbation du BT.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
SR-175	Sécurité de la virtualisation et de l'infrastructure Segmentation	Les applications, le système et les composantes de réseau (physiques et virtuels) partagés, qu'ils soient gérés par l'entrepreneur ou lui appartiennent, devrait être conçus, développés, déployés et configurés de manière à séparer convenablement l'accès usager du fournisseur et du BT (locataire) de celui des autres locataires utilisateurs, selon les facteurs suivants : Politiques et procédures établies; Isolement des biens essentiels aux opérations et des données de nature délicate des utilisateurs, qui exigent des contrôles internes renforcés et des niveaux d'assurance élevés; Respect des obligations de conformité juridiques, législatives et réglementaires applicables.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-176	Interopérabilité et portabilité Virtualisation	L'entrepreneur devrait utiliser une plateforme de virtualisation reconnue par l'industrie et des formats de virtualisation normalisés (p. ex. OVF) pour assurer l'interopérabilité. L'entrepreneur devrait aussi consigner les changements personnalisés apportés aux hyperviseurs en utilisation et à tous les crochets de virtualisation propres au SGDSL qui sont disponibles aux fins des examens réalisés par le BT.	Exigences adaptées en fonction des pratiques exemplaires de l'industrie et des directives ministérielles
SR-177	Évaluation des facteurs relatifs à la vie privée	À la demande du Canada, l'entrepreneur devrait participer activement à la réalisation d'une évaluation des facteurs relatifs à la vie privée sur la solution SGDSL conformément à la Directive du SCT sur l'évaluation des facteurs relatifs à la vie privée (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308).	Adapté en fonction des pratiques exemplaires de l'industrie et des directives ministérielles.
SR-178	Protection physique et environnementale	L'entrepreneur doit : a) Filtrer les personnes avant d'autoriser l'accès au système d'information conformément à la norme du	Adapté en fonction des pratiques exemplaires de l'industrie

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		SCT sur le filtrage de sécurité (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115) ; b) réévaluer les personnes en fonction des conditions exigeant un nouveau dépistage ; et Pour les entrepreneurs étrangers, une présélection du personnel sera requise.	et des directives ministérielles.
SR-179	Protection physique et environnementale	L'entrepreneur doit : a) Satisfaire aux exigences en matière de contrôle de la sécurité du personnel, y compris les rôles et responsabilités en matière de sécurité pour les tiers fournisseurs ; b) Documenter les exigences en matière de contrôle de la sécurité du personnel ; c) Surveiller la conformité des fournisseurs ; d) assurer le filtrage de sécurité des organisations du secteur privé et des personnes qui ont accès à l'information et aux biens protégés ; et Définir explicitement les rôles et responsabilités du gouvernement en matière de surveillance et d'utilisateur final relativement aux services fournis par des tiers.	Adapté en fonction des pratiques exemplaires de l'industrie et des directives ministérielles.
SR-180	Protection physique et environnementale	L'entrepreneur est responsable du recrutement du personnel et l'entrepreneur devrait le faire : a) Tenir à jour une liste qui identifie clairement le personnel par son nom, son titre, ses responsabilités, la formation qu'il a reçue et la formation qu'il a reçue. b) Niveaux d'accès aux installations et aux systèmes tels qu'établis dans l'énoncé des travaux. c) Soumettre la liste au chargé de projet sur demande.	Tailored based on Industry Best Practices and Departmental Guidance

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		d) Conserver un dossier de l'employé qui peut démontrer que le personnel possède les qualifications nécessaires pour effectuer le travail. Ce dossier de l'employé doit être soumis au chargé de projet sur demande. e) Effectuer les vérifications suivantes dans le cadre du processus de filtrage de sécurité et fournir l'information au chargé de projet pour chaque employé qui en fait la demande i. Contrôle d'identité 1. Copies de deux pièces d'identité originales valides délivrées par le gouvernement, dont une avec photo. 2. Nom (nom de famille) 3. Prénoms complets (prénom) - souligner ou encercler le nom usuel utilisé. 4. Nom de famille à la naissance 5. Tous les autres noms utilisés (alias) 6. Changement de nom (A) Devrait inclure le nom qu'ils ont changé de nom et le nom qu'ils ont changé, le lieu du changement et l'institution a changé par le biais de 7. Sexe 8. Date de naissance 9. Lieu de naissance (ville, province/état/région et pays) 10. Citoyenneté(s) 11. État matrimoniale/union de fait (A) Situation actuelle (marié, conjoint de fait, séparé, veuf, divorcé, célibataire) (B) Tous les conjoints actuels (s'il y a lieu)	

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		(B1) Nom (nom de famille) (B2) Prénoms complets (prénom) - souligner ou encercler le nom usuel utilisé. (B3) Date et durée du mariage/union de fait (B4) Date de naissance (B5) Nom de famille à la naissance (B6) Lieu de naissance (ville, province/état/région et pays) (B7) Citoyenneté ii. Vérification de la résidence 12. Les cinq (5) dernières années de résidence en commençant par la plus récente, sans interruption dans le temps. (C) 1. Numéro d'appartement, numéro de rue, nom de rue, ville, province ou état, code postal ou code postal, pays, dates de début et de fin. iii. Vérification de l'éducation 13. Les établissements d'enseignement fréquentés et les dates correspondantes iv. Vérification des antécédents professionnels 14. Les cinq (5) dernières années d'emploi à partir du plus récent, sans interruption dans le temps. 15. Trois (3) vérifications des références d'emploi au cours des cinq (5) dernières années. v. Vérification du casier judiciaire : 16. Rapport(s) contenant toutes les condamnations pénales des cinq (5) dernières années à l'intérieur et à l'extérieur du pays de résidence du candidat.	

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		vi. Rapport de vérification de crédit, le cas échéant. a) Pendant toute la durée du contrat, fournir au chargé de projet une vérification de casier judiciaire et de crédit à jour. b) Vérifier le rapport de tout ou partie du personnel sur demande, à la discrétion de l'autorité contractante. c) conserver les documents relatifs au filtrage de sécurité dans ses dossiers et les mettre à la disposition de l'autorité contractante pour chaque employé dans le cas d'un d) Période de dix (10) ans suivant l'offre d'emploi initiale. Réévalue les personnes en fonction des conditions qui exigent un nouveau dépistage.	
SR-181	Sécurité opérationnelle	L'entrepreneur doit : a) Veiller à ce que toutes les activités menées en rapport avec les exigences en matière de sécurité et de protection de la vie privée dans l'énoncé des travaux (EDT) offrent des niveaux de protection comparables à ceux indiqués dans les politiques du GC, et respectent ou dépassent les normes de l'industrie ou les pratiques exemplaires (p. ex. ISO 27001), selon le plus élevé des deux. b) Sur demande de l'autorité contractante, fournir une preuve de conformité à la législation du pays d'exploitation qui peut inclure, mais sans s'y limiter, la conformité aux lois nationales concernant la protection de la vie privée, le respect des lois fiscales, les règlements de constitution en société et les lois du travail. c) Identifier un agent de sécurité d'entreprise (CSO) autorisé qui sera chargé de superviser les exigences en matière de confidentialité et de sécurité des renseignements personnels traités à la suite de	Tailored based on Industry Best Practices and Departmental Guidance

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		l'exécution du contrat. Cette personne sera le point de contact pour les questions de protection des renseignements personnels et de sécurité, en collaboration avec l'autorité contractante ainsi que pour travailler avec l'autorité contractante pour les demandes d'accès à l'information (AIPRP). Le CSO sera responsable de la surveillance de l'application des pratiques en matière de protection de la vie privée et de sécurité et de la réponse aux commentaires d'audit. De plus amples informations sur la nomination et les responsabilités d'une OSC sont disponibles à l'adresse suivante : https://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/roles-eng.html. d) Assigner une personne-ressource principale en sécurité des TI ayant un lien hiérarchique fonctionnel à la direction de la sécurité qui s'assurera que les fonctions suivantes sont exécutées : i. Établir et gérer le programme de sécurité des TI de l'entrepreneur dans le cadre de l'approche globale de sécurité ; ii. Identifier, définir et documenter les rôles et responsabilités en matière de sécurité des systèmes d'information iii. Faire des recommandations concernant l'approbation de tous les contrats pour les fournisseurs externes de services de sécurité des TI ; iv. Collaborer avec les gestionnaires de la prestation des programmes et des services pour s'assurer que leurs besoins en matière de sécurité des TI sont satisfaits, fournir des conseils sur les mesures de protection et les répercussions possibles des menaces nouvelles et existantes et sur le risque résiduel d'un programme ou d'un service ;	

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		v. surveiller la conformité du Ministère aux normes de sécurité ; et Établir un processus efficace pour gérer les incidents de sécurité des TI et surveiller la conformité.	

14.2 MATRICE DE TRAÇABILITÉ DES EXIGENCES RELATIVES À LA SÉCURITÉ (MTERS)

14.2.1 Conformité aux contrôles de sécurité : éléments de preuve acceptables

La présente section définit ce qui constitue une preuve acceptable de conformité aux contrôles de sécurité dans le cadre du programme d'ESA de SPAC. C'est SPAC qui décide au bout du compte si les éléments probants fournis sont suffisants pour démontrer la conformité, et qui est le principal évaluateur de la solution du SGDSL.

14.2.2 Politiques, normes et lignes directrices

Afin de démontrer qu'il se conforme aux contrôles de sécurité exigeant l'élaboration de politiques, normes ou lignes directrices, l'entrepreneur doit, dans la colonne de la matrice se rapportant aux éléments de preuve :

a) donner le nom de l'instrument de politique qui traite du sujet;
b) indiquer dans quelle section et à quelle page du document la question précise est abordée;
c) fournir à SPAC l'instrument de politique aux fins d'examen :
   I. l'instrument de politique doit aborder tous les éléments dont il est question dans la définition du contrôle de sécurité;
   II. l'instrument de politique doit offrir un niveau de détail conforme aux instruments de politique du GC et aux pratiques exemplaires de l'industrie.

14.2.3 Certification et autorisations

Dans le cas où la conformité aux contrôles de sécurité est établie au moyen d'une attestation fournie par un sous-traitant, l'entrepreneur doit fournir une copie du certificat ou du rapport de certification, par exemple une attestation de vérification d'organisation désignée de niveau « Protégé B » délivrée par SPAC.

Dans le cas où la conformité aux contrôles de sécurité est établie au moyen d'autorisations de sécurité accordées aux employés concernés, l'entrepreneur doit fournir :

a) la liste exhaustive des autorisations accordées aux employés concernés;
b) le nom de l'organisation ayant accordé l'autorisation de sécurité;
c) le numéro de dossier, la date d'entrée en vigueur et la date d'expiration de l'autorisation.

14.2.4 Exemples d'éléments de preuve

a) paramètres de configuration;
b) documents relatifs à la conception du système;
c) diagramme présentant l'architecture ou la topologie du système;
d) captures d'écran des fonctions définies;

e) listes des contrôles d'accès;
f) plan de gestion des configurations;
g) manuel de formation et de sensibilisation en matière de sécurité;
h) registre des risques;
i) rapport d'audit;
j) rapport d'évaluation des vulnérabilités;
k) rapport sur les tests de pénétration;
l) analyse des répercussions sur les opérations (ARO);
m) titres des produits livrables associés au contrat, p. ex. plan de continuité des services de TI et de reprise après sinistre;
n) présentations;
o) captures d'écran.

14.2.5 Exemple de matrice de traçabilité des exigences relatives à la sécurité

Colonne	Titre	Description
1	ID Sec	Identificateur unique d'exigence de sécurité – à des fins de référence et de suivi
2	Contrôle de sécurité	Famille de contrôles de sécurité ou nom du contrôle de sécurité
3	No du contrôle de sécurité	Numéro du contrôle de sécurité
4	Description	Description du contrôle de sécurité
7	Éléments de preuve	Démonstration de la conformité aux contrôles de sécurité