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

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

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

Title - Sujet
Linguistic Management System

Solicitation No. - N° de l'invitation EN578-170004/B	**Date** 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 006ee.EN578-170004	**CCC No./N° CCC - FMS No./N° VME**

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: Dhir, Shaveta	**Buyer Id - Id de l'acheteur** 006ee
Telephone No. - N° de téléphone (613) 720-9354 ( )	**FAX No. - N° de FAX** ( ) -

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

Instructions: See Herein

Instructions: Voir aux présentes

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**

Canada

REQUEST FOR PROPOSAL

FOR

LINGUISTIC SERVICES REQUEST MANAGEMENT SYSTEM (LSRMS)

FOR

TRANSLATION BUREAU

REQUEST FOR PROPOSAL

LINGUISTIC SERVICES REQUEST MANAGEMENT SYSTEM (LSRMS)

TABLE OF CONTENTS

REQUEST FOR PROPOSAL

LINGUISTIC SERVICES REQUEST MANAGEMENT SYSTEM (LSRMS)

FOR

TRANSLATION BUREAU

PART 1 - GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Annexes include the Statement of Work, the Basis of Payment, Security Requirements, the Security Requirements Checklist, the Electronic Payment Instruments, the Federal Contractors Program for Employment Equity - Certification, the Insurance Requirements, the Task Authorization Form 572 and any other annexes.

1.2 Summary

1.2.1 Public Works and Government Services Canada (PWGSC) is seeking, on behalf of the Translation Bureau, a secure and complete Linguistic Services Request Management System (LSRMS) Solution to perform and manage Government of Canada’s end-to-end translation and interpretation services, processes and activities in an integrated way with Protected B security level classification for information and assets, and to provide the Government of Canada with the business intelligence, support, training it requires to ensure client service excellence.

The Translation Bureau is key to the federal government as it provides a variety of linguistic services across three lines of business which includes Translation, Terminology and Interpretation to both internal and external clients Parliament, the judiciary, federal departments and agencies, and academia. It is also the terminology authority within Government of Canada (GC) and has been mandated to develop terminology uniformity to ensure clear, consistent and quality communications within government.

The LSRMS Solution must be a Contractor Managed Service which uses provider's applications hosted on Contractor or Subcontractor infrastructure, that is secure, is working, is complete, is bug free, and is entirely hosted in Canada which includes Contractor or Subcontractor data centers, the underlying service infrastructure, network, database, web, application servers, operating systems, virtual machines, and storage.

The Contractor must host, deliver, configure, test, implement, interoperate, support, and manage a French and English Linguistic Services Request Management System Solution to the Translation Bureau.

The LSRMS Solution core functionalities must include the following:

a) Portal for the Translation Bureau resource(s), clients, external Linguistics Service Providers;
b) Workflow management;
c) Workload management;
d) Terminology management;
e) Computer Aided Translation (CAT) tools;
f) Quality Assurance tools;
g) Analytics, Reporting and Auditing;
h) Financial management interoperability;
i) Security management;
j) Scalability management; and
k) Document management.

1.2.2 There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website*.*

1.2.3 The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), and the Canadian Free Trade Agreement (CFTA).

1.2.4 This bid solicitation is to establish a contract with task authorizations for the delivery of the requirement detailed in the bid solicitation to the Identified Users across Canada, excluding locations within Yukon, Northwest Territories, Nunavut, Quebec, and Labrador that are subject to Comprehensive Land Claims Agreements (CLCAs). Any requirement for deliveries within CLCAs areas within Yukon, Northwest Territories, Nunavut, Quebec, or Labrador will have to be treated as a separate procurement, outside the resulting contract.

1.2.5 The Federal Contractors Program (FCP) for employment equity applies to this procurement; refer to Part 5 – Certifications and Additional Information, Part 7 - Resulting Contract Clauses and the annex titled Federal Contractors Program for Employment Equity - Certification*.*

1.2.6 This bid solicitation allows bidders to use the epost Connect service provided by Canada Post Corporation to transmit their bid electronically. Bidders must refer to Part 2 entitled Bidder

Instructions, and Part 3 entitled Bid Preparation Instructions, of the bid solicitation, for further information.

1.3. Multiple RFP Releases

1.3.1 Canada is releasing the Linguistic Services Request Management System (LSRMS) Request for Proposal (RFP) in three consecutive Releases, but with one bid solicitation closing date. The objective is to provide the Bidder with sufficient notice to start preparing the bid, as it will be outlined in the Bid solicitation.

The following explains the content of each RFP Release:

RFP Part 1 Release contains:

- RFP Part 1 - General Information;
- RFP Part 2 - Bidder Instructions;
- Annex A - Statement of Work (SOW);

RFP Part 2 Release contains:

- RFP Part 7- Resulting Contract Clauses

RFP Part 3 Release contains:

- RFP Part 3 – Bid Preparation Instructions;
- RFP Part 4 – Evaluation Procedures and Basis of Selection;
- RFP Part 5 – Certifications;
- RFP Part 6 – Security and Financial Requirements.
- Evaluation Plan and Methodology

Canada reserves the right, in its sole discretion, to modify the sequence, the content and the dates of the RFP releases; as well as the number of releases related to this RFP.

1.4. Debriefings

1.4.1 Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

The Contracting Authority for this solicitation is:

Name:	Shaveta Dhir
Title:	Supply Specialist
Organization:	Public Services and Procurement Canada
Address:	10 Wellington, 4th Floor Gatineau, QC K1A 0S5
Telephone:	(613) 720-9354
E-mail address:	shaveta.dhir@tpsgc-pwgsc.gc.ca

1.5. Communications Notification

1.5.1 As a courtesy, the GC requests that successful Bidders notify the Contracting Authority in advance of their intention to make public an announcement related to the award of the contracts.

1.6. Conflict of Interest

1.6.1 Bidders are advised to refer to Conflict of Interest provisions at section 18 of SACC 2003, Standard Instructions – Goods or Services – Competitive Requirements (dated 2018-05-22) and Conflict of Interest provisions of SACC 2035, General Condition – Higher Complexity – Services (dated 2018-06-21) available on the PWGSC Website https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual

1.6.2 Without limiting in any way the provisions described in 1.6.1 above, Bidders are advised that Canada has engaged the assistance of the following private sector contractor(s) and resource(s) who have provided services including the review of content in preparation of this RFP and/or who have had, or may have had, access to information related to the content of the RFP or other documents related to the LSRMS solicitation:

S.I Systems
Suite 350
1600 Carling Avenue
Ottawa, Ontario, K1Z 1G3

IBISKA
1500-130 Albert St,
Ottawa ON K1P 5G4

CGI Information Systems and Management Consultants Inc.
1410 Blair Place, 6th Floor,
Ottawa, ON K1J 9B9

TRM Technologies
280 Albert St.,
Ottawa ,ON
K1P 5G8

Any bid that is received from one of the above-noted suppliers, whether as a sole Bidder, joint venture or as a sub-contractor to a Bidder; or for which one of the above-noted resources provided any input into the bid, will be considered to be in contravention of the Conflict of Interest clauses identified in subsection 1.6.1, and the bid will be declared non-responsive.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

2.1.1 All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

2.1.2 Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

2.1.3 The 2003 (2018-05-22) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

2.1.4 Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days
Insert: 200 days

2.2 Submission of Bids

2.2.1 Bids must be submitted to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated in the bid solicitation.

2.2.2 Unless specified otherwise in the bid solicitation, bids may be submitted by facsimile. The only acceptable facsimile number for responses to bid solicitations issued by PWGSC headquarters is 819-997-9776.

2.2.3 Unless specified otherwise in the bid solicitation, bids may be submitted by using the epost Connect service provided by Canada Post Corporation. The only acceptable email address to use with epost Connect for responses to bid solicitations issued by PWGSC headquarters is: tpsgc.dgareceptiondessoumissions-abbidReceiving.pwgsc@tpsgc-pwgsc.gc.ca.

2.3 Former Public Servant

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPSs, bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada’s request and meet the requirement within the prescribed time frame will render the bid non-responsive.

Definitions

For the purposes of this clause,"former public servant" is any former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

a. an individual;
b. an individual who has incorporated;
c. a partnership made of former public servants; or
d. a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act* , 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11, the *Members of Parliament Retiring Allowances Act*, R.S. 1985, c. M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, c. C-8.

Former Public Servant in Receipt of a Pension

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:

a. name of former public servant;
b. date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder’s status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

Work Force Adjustment Directive

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information:

a. name of former public servant;
b. conditions of the lump sum payment incentive;
c. date of termination of employment;
d. amount of lump sum payment;
e. rate of pay on which lump sum payment is based;
f. period of lump sum payment including start date, end date and number of weeks;
g. number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes.

2.4 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than 10 calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as “proprietary” will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario*.*

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidders.

2.6 Improvement of Requirement During Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority at least 15 days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

ANNEX A

STATEMENT OF WORK

Linguistic Services Request Management System (LSRMS)

CONTENTS

1 LINGUISTIC SERVICES REQUEST MANAGEMENT SYSTEM (LSRMS)

1.1 Summary

The Contractor must host, deliver, configure, test, implement, interoperate, support, and manage a French and English Linguistic Services Request Management System (referred to as ***LSRMS Solution***) to PSPC's Translation Bureau.

The ***LSRMS Solution*** must be a Contractor Managed Service which uses provider's applications hosted on Contractor or SubContractor infrastructure, that is secure, is working, is complete, is bug free, and is entirely hosted in Canada which includes Contractor or SubContractor, data centers, the underlying service infrastructure, network, database, web, application servers, operating systems, virtual machines, and storage.

All data and information that is migrated, archived, backed up, stored on media, created and or associated to the ***LSRMS Solution*** will reside and remain the property of Canada at all times and as such will be required to be encrypted based on Government of Canada (GC) Security requirements. The format of the data must remain in its native format and must not be converted to a proprietary format as Canada must have the ability to access its data at any time.

The **LSRMS** ***Solution*** provided to the **Client** by the Contractor must use the applications running on the Contractor Managed service infrastructure, be secure, Web Based, and accessible from TB client devices through a web browser that is supported by GC. It is not required that the features and functionalities be provided natively within one application, however, the Contractor must ensure the applications are integrated seamlessly.

The Contractor must configure the ***LSRMS Solution*** to ensure compliance with the legislative, regulatory and policy requirements of GC as outlined in Part 2.

The LSRMS solution must be capable of interoperating with other systems, and tools that will be determined by PSPC in collaboration with the Contractor.

The Contractor must deploy a ***LSRMS Solution*** that is flexible, scalable and adaptable which will result in minimal enhancement costs to PSPC's Translation Bureau to adjust and deploy. Design, Configuration, development and implementation of the ***LSRMS Solution*** are to be with sufficient oversight by the **Client** to assure the Contractor is proceeding on schedule, and that the ***LSRMS Solution*** will be compliant with the PSPC's Translation Bureau requirements as stated in the SOW.

The ***LSRMS Solution*** must provide the features and functionalities necessary to perform and manage PSPC's Translation Bureau end-to-end Translation, Terminology and Interpretation services, processes, task and activities supporting the TB client service requests that have a GC security classification level up to Protected B (refer to *Appendix A – Glossary* for GC security classifications).

The ***LSRMS Solution*** must comply with (refer to *Section 1.3 – Scope of The Work* for details):

a) Canada's Official Languages.
b) GC IT Security standards and Security Control Profiles (SCP).

The ***LSRMS Solution*** core functionalities to be included (refer to *Section 1.3 – Scope of The Work* for details):

a) Portal for the Translation Bureau resource(s) , TB clients , external Linguistics Service Providers,
b) Workflow management,

c) Workload management,
d) Terminology management,
e) Computer Aided Translation (CAT) tools,
f) Quality Assurance tools,
g) Analytics, Reporting and Auditing,
h) Financial management interoperability,
i) Security management,
j) Scalability management,
k) Document management.

In addition, the Contractor will be required to establish and maintain a French and English service desk located in Canada (see section 5.5 for additional details) for PSPC Translation Bureau technical support requests. The Contractor will be the single point of contact for all issues related to the ***LSRMS Solution*** including any issues arising from SubContractor.

The Contractor must also deliver the documents, plans, security assessment and reports as described in this SOW.

1.2 BACKGROUND

The Translation Bureau (Bureau) is key to the federal government as it provides a variety of linguistic services across three lines of business which includes Translation, Terminology and Interpretation to both internal and external TB clients Parliament, the judiciary, federal departments and agencies, and academia. It is also the terminology authority within GC and has been mandated to develop terminology uniformity to ensure clear, consistent and quality communications within government. The linguistic management and services program is mandated under the *Translation Bureau Act*. Also, the Translation Bureau operates in a complex financial environment: revolving fund, appropriation, and special purpose allotment.

The Bureau manages/provides the translation of more than 350 million words on behalf of departments and agencies, more than 44 million words for Parliament, representing approximately 75% of the total GC spend. The Bureau also provides interpretation services for more than 5,000 days/interpreter in Parliamentary meetings and 7,000 days/interpreter for conferences.

The Bureau guarantees its TB clients quality products and as such applies rigorous quality control processes, including revision and proofreading. To provide its services, the Bureau relies on an extensive pool of internal and external translators, terminologists, and interpreters, supported by an intricate web of specialized resource(s) such as desktop publishing technicians, reference library technicians, professional support officers, file management clerks, business analysts and trainers.

The Bureau currently uses a combination of standalone internal and commercial tools to manage, track, and execute work. The current technology supporting these functions is outdated and is no longer sustainable nor scalable and very expensive to support. The current workflow involves too many manual interventions, which creates inefficiencies and higher risks of errors. From a TB client perspective, the Bureau operates a 24/7 and as such it is more difficult to support the TB clients without a self-service model or automated functionality. ***Suppliers*** (Linguistics Service Providers translators and interpreters) currently do not have access to the Bureau's systems, to communicate between the Bureau and ***Suppliers*** email is used which creates a high volume of unnecessary traffic. Translation and reference documents are dispersed and not centrally located which makes it even more difficult to ensure consistency and quality.

In an effort to optimize the PSPC application portfolio and reduce associated maintenance and support costs, the PSPC reference architecture identifies target solutions to address key business requirements. The ***LSRMS Solution*** is the target COTS solution to address requirements for business process automation and TB client relationship management for the Translation Bureau. It aims to achieve the following outcomes:

a) Standardize and streamline business processes;

b) Solution must be aligned with industry best practices for translation, interpretation and terminology management.

c) Simplify and modernize its service offering by leveraging the technology to facilitate everyday work and increase efficiency;

d) Allow e-enablement (provision of a service that can be completed online from end-to-end, except in circumstances where it is prohibited by law or security considerations of the services) at key TB client interaction points: account registrations, authentication, application, decision, and issuance of service and issue resolution/feedback (refer to Policy on Service).

e) Optimize and automate the request management to better distribute workload, increase productivity and make better use of internal and external resource(s) to perform the work;

f) To automate, track and report on the TB client billing for the work performed and similarly for freelancer invoice payment for services rendered; and

g) Provide flexibility to expand and address additional requirements and further reduce the number of legacy applications.

1.3 SCOPE OF THE WORK

The scope of the project is the hosting, delivery, configuration, testing, implementation, interoperability, support, and management of a Contractor Managed Service which uses provider's applications hosted on Contractor or SubContractor infrastructure for a Linguistic Service Request Management System (LSRMS) available in English and French. This will include enabling all the components of the ***LSRMS Solution*** that has passed full User acceptance testing by the lines of business, has been piloted with a set of Users, and has gone live followed by a complete or incremental rollout that may also include running both legacy and new ***LSRMS Solution*** for a period of time and be determined by PSPC in collaboration with the Contractor.

This project includes project management activities, security assessments, data migration, business continuity and disaster recovery, maintenance and support and training. The Bureau will require French and English support from the Contractor and the Contractor may be called upon to provide professional services, on and as when requested basis, through task authorizations, as part of the contract.

The ***LSRMS Solution*** must be compliant with GC Acts and standards:

a) ***Canada's Official Languages***: Must comply with Canada's Official Languages Act and provide User with the choice of operating in the language of their choice English or French.

b) **GC Security:** Must comply with the GC IT Security guidelines and the Security Control Profiles (SCP) outline in Appendix G.

The ***LSRMS Solution*** must be and include:

c) Contractor Managed Service**:** The ***LSRMS Solution*** must be a Contractor Managed Service which uses provider's applications hosted on Contractor or SubContractor infrastructure, that is secure, is working, is complete, is bug free, and is entirely hosted in Canada which includes Contractor or SubContractor data centers, the underlying service infrastructure, network, database, web, application servers, operating systems, virtual machines, and storage.

d) Data: All data and information that is migrated, archived, backed up, stored on media, created and or associated to the ***LSRMS Solution*** will reside and remain the property of Canada at all times and as such will be required to be encrypted based on Government of Canada Security requirements. The format of the data must remain in its native format and must not be converted to a proprietary format as Canada must have the ability to access its data at any time.

The Core functionalities considered to be in the scope of the ***LSRMS Solution*** are:

e) **Portal for the Translation Bureau resource(s):** Provide a customizable role based Web Based interface and access to Bureau professionals with access to ***project*** related information, scheduling, time reporting, assigned Tasks or events, ***project*** statuses and notes, TB client preferences and reference material, attachments, access to LSRMS suite of tools, and access to personal statistics, dashboard and reports based on a User's role, access rights and permission.

f) **Portal for the TB clients:** Provide a customizable self-serve Web Based interface and access to allow TB clients to submit and track the progress of the service requests (***project***) in real time throughout the workflow, upload documents and references. It will also allow TB Clients to obtain ***project*** quotes (estimates), communicate with Bureau resource(s), and provide access to linguistic information and services including financial information and TB client statistics, dashboard and reports based on access rights and permission.

g) **Portal for external Linguistics Service Providers:** Provide a customizable web-based interface and access to ***project*** related information, assigned Tasks, ***project*** statuses and notes, attachments and access to Translation Bureau request management system and computer assisted translation tools, translation memories relating to their ***projects***, TB client preferences and reference material, including personal statistics, dashboard and reports based on access rights and permission.

h) **Workflow management:** Provide Bureau professionals (project team and support, Translators, Terminologists, and Interpreters with customizable web-based tools, and technology to streamline the processes that will enable the Bureau to deliver quality products and services to the TB client more effectively. This component will provide workflow design (model current and future business processes), business rule configuration, allow User communication throughout life cycle of the request, manual and automated request (***project***) management, processing and handling of TB client service requests (***projects***) from reception to delivery and billing.

i) **Workload management:** Provide a customizable web-based interface that allows for the management of Tasks and events, planning, scheduling, and dispatching (assigning) of Bureau resource(s) based on configurable scale, attributes, and business rules. This component will also allow the management of human resource(s) and profiles which may include attributes such as role, availability, qualification, certification, language, security clearance, word translation average, translation domains and specialties (aviation terminology, medical etc.) and may include material resource(s) management such as room, venue, location and equipment (audio visual) reservations.

j) **Terminology management**: This component provides terminology databases and terminology extraction with the ability to use the Terminology product to translate recognized terms in the content, document specialized terminology and TB client terminological preferences, and create lexicons.

k) **Computer Aided Translation (CAT) tools**: This component provides pre-translation tools, analysis, editing, alignment, search engine, machine translation, the ability to manage and use the Translation Memory TM to translate content as well as the ability to manage, customize, categorize and segregate into ***project*** and general translation.

l) **Quality Assurance tools**: This component provides the ability to edit, revise, proofread, grammar and spellcheck content before and after its delivery to the TB client and/or its entry in the Terminology management or CAT tool TM in order to ensure post translation quality.

m) **Analytics, Reporting and Auditing:** Advanced analytics, reporting and auditing capabilities to provide business intelligence. This component will also allow the ability to search, filter and query the metadata and data from a variety of sources to produce customized reports, to report on transactional data, to support dashboards/scorecards (reporting on indicators, departmental and operational service standards, key performance indicators (KPIs), provide trending and analytical support.

n) **Financial management interoperability:** The ***LSRMS Solution*** will interface with the GC financial system (SIGMA) to exchange data for TB client invoicing and reporting.

o) **Security management:** Access to the ***LSRMS Solution***, suite of tools, features and functionalities against the GC IT Security Control Profiles.

p) **Scalability management:** The ***LSRMS Solution*** must provide the ability to scale up and down to cover 2000 concurrent Users at any one time, without any service degradation.

q) **Document management:** The ***LSRMS Solution*** will provide the GC with the ability to handle documents up to Government of Canada Protected "B" standards. This component should allow documents to be managed throughout the life cycle of the request from reception to delivery and final repository. It should provide document input (scanner, email, manual and auto upload), searches, indexing, versioning, processing, support a variety of formats, able to configure retention period, and apply document control and security.

1.3.1 *LSRMS Solution* Vision and Deployment Approach

The ***LSRMS Solution*** will provide significant opportunities to transform and modernize the Bureau. Introducing an enabling technology that will standardize, optimize and automate processes will allow the Bureau to shift from a focus on manually carrying out transactional requests with little value to the process, to strategic project planning. This shift will be facilitated by the introduction of online tools to enable TB clients to process standard requests with limited involvement of the Bureau employees. This allows Bureau employees to contribute their expertise to more strategic and complex activities that position the federal linguistic services program to deliver better outcomes.

In addition, the ***LSRMS Solution*** will enable the completion of translation, terminology uniformity and interpretation activities and the support thereof with a modern and integrated suite of tools in the areas of translation memory management, terminology management, and quality control, interpretation scheduling and reporting.

1.4 STRUCTURE OF THE STATEMENT OF WORK

The body of this Statement of Work (SOW) provides high level description on the structure and content of the SOW as follows:

	Title	Description
Part 1	Linguistic Services Request Management System	Provides solution summary, background, scope, Translation Bureau metrics, organization, services, workflow, SOW structure, and Common Terminology.
Part 2	Legislative, regulatory and policy requirements	Provides information on Contractor 's obligation to comply with legislation, regulations, policies, directives, standards
Part 3	Functional requirements	Outlines the requirements for the ***LSRMS Solution*** and its components.
Part 4	Technical requirements	Outlines the Technical requirements for the ***LSRMS Solution*** and its components.
Part 5	Non-functional requirements	Provide information on high level commitment, security requirements, communication, service management and web accessibility.
Part 6	Management and oversight	Details on the milestones, deliverables and security requirements.
Part 7	Professional services	Outlines the Contractor professional service resource(s) that may be required for additional work and customisation of the ***LSRMS Solution***.
Part 8 - Appendix A	Glossary	Defines terminology used in this SOW.
Part 9 - Appendix B	Acronyms	Defines acronyms and abbreviations used in this SOW.
Part 10 - Appendix C	Translation Bureau Reports	List of potential Bureau reports.
Part 11 - Appendix D	Professional Service resource(s) Responsibilities	List of Contractor resource(s) that may be required for the ***LSRMS Solution***.
Part 12 - Appendix E	Interpretation Workload Calculations	This part outlines the information used to calculate the total number of hours worked by Conference and Parliament interpreter employees.
Part 13 - Appendix F	Translation Bureau Languages and File Formats	List of Translation Bureau supported languages and file formats.
Part 14 - Appendix G	Security and Privacy	ITSG-33 Security Controls LSRMS Security Control Profile (SCP) and Security Requirement Traceability Matrix information.

1.5 COMMON TERMINOLOGY

In addition to the glossary, the common and reoccurring terms herein will have the following definition and meaning.

In this SOW:

Term	Definition
Canada's Official Languages	Canada's Official Languages which are English and French.
Linguistic Service Provider (LSP)	An internal or external resource(s) that provides linguistics services for Translation, Terminology, or Interpretation.
LSRMS Solution	A comprehensive COTS solution that provides all the necessary infrastructure applications and tools including out of the box features and functionalities that allows Users, internal and external resource(s) to perform the Tasks and activities required to deliver Translation, Terminology, and Interpretation services to the TB client.
Project	A request or order submitted by a TB client to obtain a service.
Suppliers	A company that may have one or more resource(s) that can provide linguistics services to the Translation Bureau.
Web Based	Allows a User to access and interact with the solution and its applications using a web browser such as Internet Explorer, Chrome, Firefox, or Safari.
Key terms and acronyms used throughout this document may be found in *Appendix A – Glossary* and *Appendix B - Acronyms*.	

1.6 TRANSLATION BUREAU

1.6.1 Overview

The Translation Bureau handles and provides the delivery of Translation, Terminology and Interpretation services. The following tables represent a brief overview on the three Bureau lines of business outlining the services, TB clients, and languages refer to *Appendix F – Translation Bureau Supported Languages* for a complete list.

1.0 Translation	
a) Services	I. Translation, revision, editing, and others.
b) TB clients	I. Federal departments and agencies, II. Parliament (The Senate, the House of Commons, Library of Parliament, and others), and III. Private-sector firms that have a contract with the federal public service.
c) Language	I. Canada's Official Languages, II. Aboriginal, and III. Foreign languages.

2.0 Terminology	
a) Services	I. Free terminology or linguistic advice II. Customized bilingual or multilingual glossaries, and III. Terminology standardization, and others.
b)TB clients	I. Participation in the work of terminology committees, and II. Participating, at a TB client's request in terminology committees not related to the Bureau's standardization mandate and involving only one department or agency.

2.0 Terminology	
c) Language	I. Canada's Official Languages, II. Aboriginal, and III. Foreign languages.

3.0 Interpretation	
a) Services	I. Parliament Interpretation, and II. Conference and visual interpretation services.
b) TB clients	Parliament I. Debates of the House of Commons, II. The Senate and their committees, III. Cabinet and Caucus meetings, IV. Parliamentary press conferences, and V. Proceedings of the Library of Parliament and parliamentary associations. Conference and visual interpretation services I. International summits, II. Bilateral or multilateral discussions between heads of state or government, III. Intra- or inter-departmental conferences, and IV. Meetings between federal ministers and their provincial or territorial counterparts.
c) Language	I. Canada's Official Languages, II. Aboriginal, III. Foreign languages, and IV. Visual languages (visual sign and tactile languages).

1.7 VOLUMETRIC DATA

The volumetric data in this Statement of Work is based on limited statistical information due to the reporting limitations of the legacy systems currently in place. The statistics are provided for information purposes only

a) Number of Active and Inactive TB client (Parent) and TB Sub-client (Child) accounts:

TB client **Account Code (XXX-XX-XX)**		**Number of TB** clients **2017-2018**		
Account Structure	**Example**	**Active**	**Inactive (within 12 months)**	**Total**
Primary level (Parent) – Department	Public Services and Procurement Canada	248	230	**478**

Secondary level – Branch	Translation Bureau	1428	962	**2390**
Tertiary level – Directory or Section	Strategic Reengineering	9242	7159	**16401**

b) Volume of Words and Events (2016-2017):

Words	Volume
Words translated per year	> 310 million words

Events		Volume
Parliamentary interpretation events	Official and aboriginal languages (on demand)	~ 5040
Conference interpretation events	Official and aboriginal languages	1801
	Foreign languages	382
Visual Interpretation events	Langue des signes québécoise (LSQ), American Sign Language (ASL), English and French oral (lip-reading) interpreting, Deaf-blind intervenor (tactile interpreting)	1577

c) Number of Linguistic Service Providers (LSP) for Translation and Interpretation (2016-2017):

Linguistic Service Providers (LSP)		Number
Internal translator	Official and foreign languages	895

Linguistic Service Providers (LSP)			Number
Internal interpretation	Parliamentary	Official languages	39
	Conference	Official and foreign languages	25
External (LSP) interpretation	Parliamentary	Official languages	30
		Foreign and aboriginal languages	~ 10 to 15
	Conference	Official and aboriginal languages	145
		Foreign languages	160
	Visual	Langue des signes québécoise (LSQ) American Sign Language (ASL) English and French oral (lip-reading) interpreting Deaf-blind intervenor (tactile interpreting)	~ 150

d) There are many databases used in the Translation Bureau, two of which have significant importance in the day to day operation. The first is known as "Bio Corpus" which is a repository for the complete formatted source document and the final formatted target document. The second is known as "Mega

Corpus" which is the Translation Memory repository for all translation segments, paired and aligned used by the Translation Bureau resource(s).

The following table shows the capacity, used, remainder, and percent change year to year:

Database Name	Capacity	Used	Remainder	Percent Change Year to Year
Bio Corpus	1.0 TByte	968 GB	32 GB	~ 16 %
Mega Corpus	481 GB	279 GB	175 GB	~ 16 %
TByte = Terabyte, GB = Gigabyte				

1.8 TRANSLATION BUREAU'S SECTORS, BUSINESS FUNCTION AND KEY ACTIVITIES

The Translation Bureau has several sectors comprised of the Contact Centre (CC), Request Processing Centre (RPC), Translation & Terminology Centre (TTC), Professional Support Centre (PSC), and Service to Parliament, Conference and Visual Interpretation. The Bureau handles and provides the delivery of Translation, Terminology and Interpretation services to its TB clients with each of the sectors having different core business functions and operation.

The following table is a list of the Bureau sectors, business function and key activities:

1.0 Contact Centre (CC)			
1.1	**Business Function**	a) To receive and process requests for information and services from TB client, ***Suppliers***, employees and the general public.	
1.2	**Key Activities**	a) Receiving all calls made and emails sent to the Translation Bureau's generic points of contact by TB client, ***Suppliers***, employees and the general public, b) Processing and closing general requests in accordance with established service standards, c) Forwarding complex requests to the appropriate Centres of Expertise.	

2.0 Request Processing Centre (RPC)			
2.1	**Business Function**	a) To assess the linguistic services workload, dispatch work to ***Suppliers*** and internal resource(s) and monitor workload progress.	
2.2	**Key Activities**	a) Assessing service requests from TB clients, b) Creating and coordinating estimates, c) Planning and coordinating work, d) Dispatching work to ***Suppliers*** and internal resource(s) , e) Monitoring requests in all stages, from reception to delivery, f) Assessing external contract capacity.	

3.0 Translation & Terminology Centre (TTC)		
3.1	**Business Function**	a) Provide translation and terminology products and services to Parliament, the judiciary and federal departments and agencies in both official languages, in visual languages and in other languages, b) To provide these services, upon request, to other governments in Canada and to international organizations, c) To standardize the terminology used in the federal government.
3.2	**Key Activities**	a) Delivering translation and revision services internally and by ***Suppliers***, b) Evaluating ***Suppliers***' work, c) Standardizing terminology, d) Producing terminology bulletins, glossaries and vocabularies, e) Managing the Translation Bureau's terminology databases, f) Quality assurance.

4.0 Professional Support Centre (PSC)		
4.1	**Business Function**	a) To provide professional support services to the Translation Bureau's clients, ***Suppliers*** and internal language professionals.
4.2	**Key Activities**	a) Handling terminology and documentation requests from ***Suppliers*** and internal resource(s) , b) Managing and updating the library catalogue and reference kits for Bureau translators and ***Suppliers***, c) Rereading terminological records before they are published d) Carrying out automatic extraction and terminology scanning and writing draft records, e) Formatting documents to ensure correct presentation, f) Delivering transcription services to TB clients and members of the organization g) Proofreading documents before they are delivered, h) Processing working documents from the Request Processing Centre, i) Managing the content of translation memories, j) Delivering documents.

5.0 Service to Parliament, Conference & Visual Interpretation		
5.1	**Business Function**	a) To provide interpretation services to Parliament, the judiciary and federal departments and agencies in both official languages, in visual languages and in other languages, b) To provide these services, upon request, to other governments in Canada and to international organizations, c) Accreditation for interpreters.
5.2	**Key Activities**	a) Delivering interpretation services internally and by ***Suppliers*** (LSP), b) Evaluating ***Suppliers***' work.

The resource(s) within each sector can have one or multiple roles assigned to them depending on the nature of the work that is required to meet the core business function. These roles are usually associated with Tasks and activities, once assigned they can provide the access rights and permission to the features and functionalities of the tools needed to complete the Tasks and activities.

1.9 TRANSLATION BUREAU'S SERVICES

The following is a list of the Bureau's services currently provided:

Services	Description
Adaptation	Translating a document and making changes to tailor the message to its target audience.
Administrative services	Handling a request that requires an unusual amount of administrative processing. For example, handling a request of many files, processing files that are complex and/or that require extra processing (such as PDF and JPG files), merging files, and searching for documents that have already been translated.
After-Hours Emergency Service	Providing translation or linguistic services outside regular business hours, on weekends and on statutory holidays.
Conference interpretation	Providing conference interpretation services in official, Aboriginal, foreign and visual/sign languages.
Comparative revision	Carefully comparing a translation with the original text and correcting the content and style of the translation.
Editing (unilingual)	Improving an original text by correcting the grammar or style or by suggesting solutions to make the text easier to read and understand.
Editing (unilingual) and translation	Editing an original document and then translating it.
Editing (unilingual) and translation of a bilingual document	Editing a document that has text in two languages and then translating the document into each of the two languages.
Editing (unilingual), translation and comparative revision	Editing an original document, translating it, and then doing a detailed comparison of the original text with the translation in order to correct the content and style of the translation.
On-site translator	Providing the services of a language professional who can work exclusively and autonomously for a TB client or a group of TB clients in their offices or, in exceptional circumstances, in our offices.
Parliamentary interpretation	Providing official languages interpretation services to Parliament.
Professional evaluation	Assessing in detail the quality of translations, revisions, or any text written in English or French, using recognized criteria that ensure fairness and objectivity. The assessment is presented either as a detailed report (with supporting examples) or as brief comments on each text.
Project management	Planning, organizing, directing, controlling and monitoring a complex linguistic or translation ***project***.
Proofreading	Reading a text, identifying any errors or typos, and indicating any changes to be made.

Services	Description
Revision of a bilingual document	Editing a document that has text in two languages.
Sight translation	Translating a document orally, either in person or by telephone.
Summary	Giving an oral or written summary of a document in the same language or in another language.
Terminology services	Developing customized glossaries, participating on behalf of TB clients in terminology committees and other terminology ***projects.***
Translation	Rewriting a text in another language, taking into account the tone, style and terminology used by the author.
Translation and comparative revision	Translating a document and then having the translation revised by another professional. Recommended for documents that are to be read by a high-profile public or the general public or for documents that will have a wide readership or a significant impact.
Translation of a bilingual document	Translating a document that has text in two languages.
Translation of modified documents	Translating changes made to a text that has already been translated.
Translator on standby	Providing the services of a language professional who can be reached on short notice at any time for a specific period to carry out a TB client's work. The translator can, however, carry out other activities during this time.
Writing assistance	Drafting a text in collaboration with a TB client and providing linguistic advice on translation problems and language issues (grammar, style, punctuation, terminology, etc.).

1.10 TRANSLATION BUREAU WORKFLOW

1.10.1 Overview

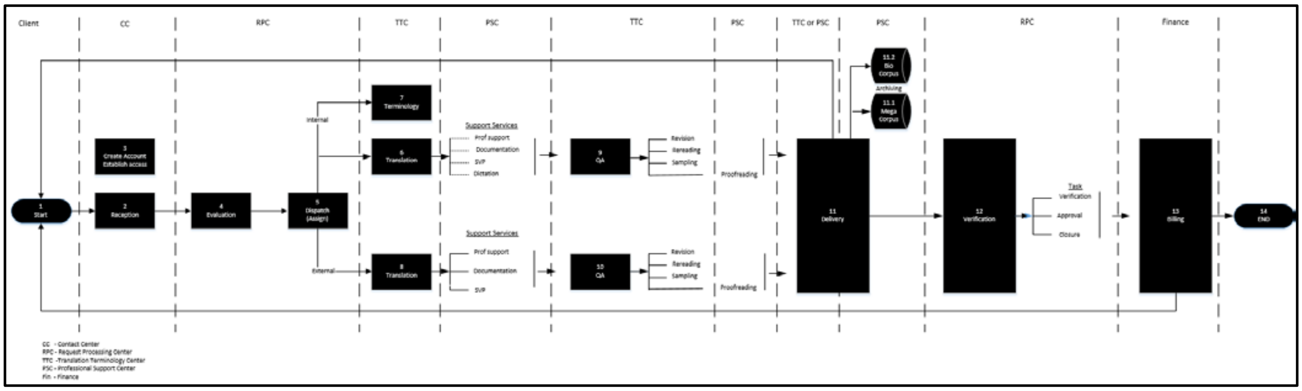
The Bureau has a number of workflows that are used to deliver Translation, Terminology, and Interpretation services to the TB clients. The workflows are comprised of many branches containing a variety of Tasks and activities based on the services requested.

As part of the ***LSRMS Solution***, workflow management is an essential component and is tightly coupled with the functional requirements in this Statement of Work such as; workload management, TB client and resource(s) portals, TB client and resource(s) profiles, analytics, reporting and business intelligence. The workflow management component features and functionalities working in unison with the other requirements, would allow the Bureau to reduce manual intervention, to automate and manage more efficiently and effectively the services, TB client requests, internal and external resource(s), workload, Tasks, and activities in delivering quality services.

To provide an example of the current Tasks and activities used in the Bureau, a high level summary of a Translation workflow is included below. It is important to note that at the time of this writing the other workflows pertaining to Terminology and Interpretation (Parliamentary, Conference, and Visual) were work in progress and not readily accessible. Once completed they can be made available upon request

1.10.2 Translation Workflow

The following is a high level Translation workflow from TB client submission of service request to delivery;



1.10.2.1 High Level Translation Workflow Details

The table below identifies at a high level the current actors, task, activities, and description in the Translation workflow;

Number	Actor	Task/ Activity	Description
1	TB client	Start	The TB client submits their request through the Translation Bureau (TB) system. Additionally, the request may be submitted by e-mail or other means if the TB client does not have access to the system or if the security of the documents does not allow them to attach the request.
2	CC	Reception	The TB receives the TB client's request through the TB system or by email or other means. It downloads the documents to be translated and the reference documents. It analyzes these documents to evaluate the word count and compares them with the content of the Translation Memory (TM).
3	CC	Create account Establish access	Two types of accounts must be created to use the system: 1. The TB client-account must be created beforehand. Billing information must be entered at the client account level. 2. The TB client must have a User account. User accounts are unique and are linked to a TB client account. Multiple Users can be associated with a TB client account.
4	RPC	Evaluation	The TB evaluates the TB client's request and validates the requested service and the due date. After

Number	Actor	Task/ Activity	Description
			consultation with the TB client, the advisor modifies the request if necessary.
5	RPC	Dispatch (Assign)	The request is divided according to its domain, language and time. The request is split into slices if it is too large for a single translator to meet the deadline.
6	TTC	Translation	A TB translator performs the translation of the document.
6	PSC	Support Services	The professional support center offers several services that allow translators to devote themselves to translation. These services are: professional support (encryption, document conversion, and others), documentary services, publishing and transcription to name a few.
7	TTC	Terminology	Translators have access to customer-specific terminology kits to standardize vocabulary, acronyms and other relevant customer information. The terminology kits are maintained by TB content specialists.
8	TTC	Translation	An external linguistics service provider translates the document.
8	PSC	Support Services	The professional support center offers several services to external linguistics service provider to enable them to meet certain standards and standardize the TB client's translation. These services are: professional support (encryption, document conversion, and others), documentary services and desktop publishing, to name just a few.
9	TTC	QA	An internally translated text is reviewed or re-read according to the nature of the document. It may also be subject to proofreading if the translator so wishes and time permits.
10	TTC	QA	For an external linguistics service provider a translated text is reviewed or re-read according to the nature of the document. If the nature of the document does not require revision or re-reading, it must pass through the sampling process before being subjected to proofreading before delivery to the TB client.
11	TTC or PSC	Delivery	Delivery of translated documents to TB client.
11.1	PSC	Archiving – Mega Corpus	The Mega Corpus contains archival documents (source and translated documents) segmented and indexed for use by TB's search engines.
11.2	PSC	Archiving – Bio Corpus	The Bio Corpus contains all the archival documents (source and translated documents) of the TB in their original formats. Bio Corpus is used to power the Mega Corpus

Number	Actor	Task/ Activity	Description
12	RPC	Verification	Verification of Tasks and units to bill for the billing (invoicing) process.
13	Finance	Billing	This process is run twice a month according to an established schedule. The TB system calculates the invoices and generates an output that is sent to SIGMA (SAP). Once data is processed in SIGMA, a file is generated by SIGMA and uploaded to the TB system to match the billing information between the TB system and SIGMA.
14	END	END	The request was processed, delivered and invoiced.

2 LEGISLATIVE, REGULATORY AND POLICY REQUIREMENTS

2.1 INTRODUCTION

The ***LSRMS Solution*** must enable GC's compliance with all its legislation, regulations, policies, directives, standards and guidelines as detailed below. The ***LSRMS Solution*** must comply with all legislation, regulations, policies, directives, standards and guidelines.

Ensuring the security and protection of personal information remains a priority for PSPC and ***LSRMS Solution*** and Contractor must adhere to all relevant legislation including but not limited to those related to privacy and the handling and storage of personal information.

2.2 LEGISLATION, REGULATIONS, POLICIES, DIRECTIVES, STANDARDS AND GUIDELINES

The Contractor and ***LSRMS Solution*** must comply with GC legislation, regulations, policies, directives, standards, guidelines, and specifications such as but not limited to:

Type	Name	URL
Policy	Policy on Privacy Protection	*https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510*
	Policy on Government Security	*https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578*
	Implementing HTTPS for Secure Web Connections: Information Technology Policy Implementation Notice (ITPIN)	https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/implementing-https-secure-web-connections-itpin.html
	Direction for Electronic Data Residency	https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/direction-electronic-data-residency.html
Act	Official Languages Act	*http://laws-lois.justice.gc.ca/eng/acts/O-3.01/index.html*
	The Privacy Act	*http://laws-lois.justice.gc.ca/eng/acts/p-21/*
	Personal Information Protection and Electronic Documents Act (PIPEDA)	*http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html*
	Management of Information Technology Security (MITS) standard	*http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328*
Guidelines	ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada	https://www.cse-cst.gc.ca/en/node/268/html/28461

Type	Name	URL
	ITSG-33 IT Security Risk Management: A Lifecycle Approach (through compliance with the SCP)	*https://www.cse-cst.gc.ca/en/publication/itsg-33*
	ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones	https://www.cse-cst.gc.ca/en/node/266/html/27445
	ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information	https://www.cse-cst.gc.ca/en/publication/list/Cryptography
	ITSP.30.031 V3 User Authentication Guidance for Information Technology Systems	https://www.cse-cst.gc.ca/en/node/2454/html/28582
	ITPIN: 2014-01 Security Considerations for the Use of Removable Media Devices for Protected C and Classified Information	https://www.cse-cst.gc.ca/en/node/1224/html/2269
	RCMP G1-001 Security Equipment Guide	http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/home_e.htm
Standards	WCAG2.0 Accessibility	http://www.w3.org/TR/WCAG20/
Specification	CVSS v3.0 Common Vulnerability Scoring System v3.0	https://www.first.org/cvss/specification-document

All federal legislation, including those not listed above, can be found in their entirety on the Department of Justice website: www.justice.gc.ca.

3 FUNCTIONAL REQUIREMENTS

3.1 INTRODUCTION TO THE FUNCTIONAL REQUIREMENTS

The functional requirements specify the scope of work including specific activities to be performed by the Contractor, as well as overall capabilities that the ***LSRMS Solution*** must include while adhering to applicable legislative and policy mandated requirements specific to each sub-activity. The Contractor must perform the following activities and provide an ***LSRMS Solution*** that includes:

a) Customizable web-based and interactive tool that can be readily configured by User to reflect their specific requirements.
b) Allow for the definition of User roles, access rights and permission for the solution, suite of tools, features and functionalities.
c) Have workflow and business rules to be configured by User to support a wide variety of processes, activities and functions.
d) Allow for the effective management of the metadata and data for example any and all data will be entered once and validated within the solution, with the ability to re-use and leverage data throughout the solution and across its functionalities.
e) Allow for seamless data sharing within the solution and other related systems hosted by the Contractor.
f) To support the re-use of commonly required data in a secure manner across the solution and other PSPC systems.
g) Allow for constant change and real-time access to data, reporting and analytic information to support the effective management and business decision-making of the PSPC, monitoring and tracking of processes and performance.

The Contractor must fully integrate all functional requirements unless otherwise stated as described in sections A to I of *Part 3: Functional Requirements* of the SOW.

3.2 SECTION A – GENERAL REQUIREMENTS

3.2.1 Objective

The general requirements section identify high level functions and outcomes that are applicable across all elements of the ***LSRMS Solution***.

3.2.2 Requirements

SOW NUM	Requirement (MANDATORY)
GEN-SOLN-01	**Solution** The ***LSRMS Solution*** must be a Contractor Managed Service which uses provider's applications hosted on the Contractor or a SubContractor infrastructure, that is secure, is working, is complete, is bug free, and is entirely hosted in Canada which includes Contractor or SubContractor data centers, the underlying service infrastructure, network, database, web, application servers, operating systems, virtual machines, and storage.

SOW NUM	Requirement (MANDATORY)
GEN-DATA-02	**Data and Information** All data and information that is migrated, archived, backed up, stored on media, created and or associated to the ***LSRMS Solution*** must reside and remain the property of Canada at all times and as such is required to be encrypted based on GC (Government of Canada referred to as GC or Canada) Security requirements. The format of the data must remain in its native format and must not be converted to a proprietary format as Canada must have the ability to access its data at any time.
GEN-WEB-03	**Web Based** The ***LSRMS Solution*** features and functionalities for Translation, Terminology and Interpretation must be Web Based and include portals (TB client, internal and external resource(s)), dashboards, workflow, workload, terminology, security management, computer aided translation (CAT) tools, Translation memories, TermBase, analytics, reports, and business intelligence.
GEN-SIGMA-04	**Interoperability with SIGMA (SAP):** The ***LSRMS Solution*** must provide the following functionality to: a) Ensure all relevant financial information is transferred between the ***LSRMS Solution*** and SIGMA, using file import and export functionality to and from a secure landing pad. b) Ensure verification of ***supplier*** contract information from SIGMA
GEN-IMPEXP-05	**Import and Export** The ***LSRMS Solution*** must provide the following functionality: a) Import data, files, reports, analytics, query results into ***LSRMS Solution*** in various formats that includes; MS Word (doc, docx), MS Excel (xls, xlsx), txt, pdf, xml, tmx, tbx, and csv. b) Export data, files, reports, analytics, query results from ***LSRMS Solution*** in various formats that includes; MS Word (doc.docx), MS Excel (xls, xlsx), txt, pdf, xml, tmx, tbx, and csv. Note: For a list of file formats used by the Translation Bureau refer to *Appendix F - Translation Bureau Languages And File Formats.*
GEN-SFTP-06	**Secure File Transfer Protocol (SFTP)** The ***LSRMS Solution*** must support Secure File Transfer Protocol.

SOW NUM	Requirement (RATED)
GEN-SRCH-07	**Search** The ***LSRMS Solution*** should provide the functionality to search based on reportable fields, document attributes, and metadata.
GEN-USAB-08	**Usability** The ***LSRMS Solution*** should provide the functionality for a User with the proper role, access rights, and permission to be able to tailor and configure the User interface and attributes, control business behaviour (such as conditions that should be met before User can amend a service request) using business rules and input validation.
User **Interface** The ***LSRMS Solution*** should provide the following functionality;	

SOW NUM	Requirement (RATED)
GEN-INTFC-09.1	Configure the User interface by; a) Adding new attributes or modify functionality of existing attributes, b) Setting attribute types such as number, free text, pick list, and Boolean, c) Setting attribute GUI position and tab order d) Setting attribute level behaviour and properties such as labels, mouse over help, mandatory/optional, visibility, default value, e) Creating business rules and input validation. f) Setting print layout g) Specifying which data attributes are pre-populated when the artifact is created (such as prepopulate User data from the requester's User profile on a requisition when a request is created) h) Specifying the behaviour using business rules, validation rules that apply when the business process is modified. i) Tracking and be able to display changes (history) for each input and business transaction j) Modifying information, changing workflow approval or denial, changing submissions to external resource(s) , and confirmation, k) Configuring the User interface layout of a portal, l) Identifying and submitting to the Contractor changes to hard coded values, attributes, and data fields in the User interface.
GEN-INTFC-09.2	The ***LSRMS Solution*** component's interface should provide brief User instructions and tips in a consistent manner across all controls and displays.
GEN-INTFC-09.3	The ***LSRMS Solution*** component's interface should follow a standard, theme, and text tone across the component.
GEN-INTFC-09.4	The ***LSRMS Solution*** should support customizable colour selection and other visual configuration options to enable PSPC to brand the interface in accordance with PSPC standards.
Online Help The ***LSRMS Solution*** should provide the functionality to:	
GEN-HELP-10.1	Provide a configurable reference section that contains links to quick reference guides, manuals, tutorials and policies.
GEN-HELP-10.2	Provide in-application help and User support for features, functionalities and processes.
GEN-HELP-10.3	Enable presentation of context sensitive help topics aligned with the section of the ***LSRMS Solution*** the User is currently on.
GEN-HELP-10.4	The ***LSRMS Solution*** should provide a frequently asked questions function which is accessible at any time during operation, without losing the context of the current transaction, and which provides topic based navigation.
GEN-ERR-11	**Error Messages, Alerts & Notifications** The ***LSRMS Solution*** should provide and allow a User with the proper role, access rights, and permission to configure and control system error messages, alerts, notifications and their triggers.
GEN-DOC-12	**Documentation** The Contractor should provide PSPC with all documentation and collateral material that is available for the current solution and all future releases.

SOW NUM	Requirement (RATED)
Web page layouts, Templates, Forms Configuration The ***LSRMS Solution*** should provide a User with the proper role, access rights, and permission;	
GEN-CONFIG-13.1	To create and configure web page layouts, templates, and forms
GEN-CONFIG-13.2	To be able to do the following to the web page layouts, templates, and forms; a) Set fields as mandatory or optional, b) Configure and set default values for common data entry fields, c) Add User-defined fields to any screen or tabs, d) Administer existing and define new data elements with various characteristics such as business rules, predefined validation rules, value ranges, dropdown lists, free form texts with User defined length maximums, e) Configure and create different types of extrinsic fields, f) Input controls: checkboxes, radio buttons, dropdown lists, list boxes, buttons, toggles, text fields, date field, text terminal windows, g) Navigational Components: breadcrumb, slider, search field, pagination, slider, tags, icons, tabs, h) Informational components: tooltips, icons, progress bar, notifications, message boxes or windows, dialog box, modal windows (pop up), i) Menus: menu bar, menu, context menu, extra menus, primary and secondary menus, j) Modify out of the box field labels, k) Automatically notify a User of incomplete mandatory data fields, and l) Modify key performance indicators (KPIs), operational and departmental service standards which may change year to year.
GEN-PRJCT-14	**Projects (Requests)** The ***LSRMS Solution*** should provide the functionality: a) To prevent TB clients from submitting incomplete translation requests and provide information for corrective action, b) For a User with the proper role, access rights, and permission to change the request status, c) For a User with the proper role, access rights, and permission to cancel a request and send a notification to TB client, d) For a User with the proper role, access rights, and permission to manually and automatically create a quote and send to TB client.
GEN-ACCS-15	**Restrict Access** The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to restrict access to features and functionalities.
GEN-WCAG-16	**Web Accessibility** The ***LSRMS Solution*** web pages should be WCAG 2.0, Level AA compliant.

3.3 SECTION B – LANGUAGE REQUIREMENTS

As required by the *Official Languages Act*, the PSPC has an obligation to provide service delivery in Canada's Official Languages.

The Contractor must make all User-facing components of ***LSRMS Solution*** applications, services, information and tools (such as background text, web applications, error and warning messages, system tables, system generated messaging, and any print and on-line documentation) available in both of Canada's Official Languages.

The Contractor must:

a) Provide materials for any User in both official languages, including training materials.
b) Personal communications to User must be provided in the User's language of choice, if the User has not indicated a preference.
c) Maintain a record of User's language preference so that all personal communications are received in their language of choice.
d) Ensure that all User-oriented communication materials are available for distribution in both Canada's Official Languages.
e) Ensure ***LSRMS Solution*** and suite of tools is available in the official language of the User's choice.

3.3.1 Objective

The ***LSRMS Solution*** must meet the official languages obligations of the GC under the *Official Languages Act* (http://laws-lois.justice.gc.ca/eng/acts/O-3.01/index.html).

3.3.2 Requirements

SOW NUM	Requirement (MANDATORY)
LANG-01	The entire ***LSRMS Solution*** must be available in both Canada's Official Languages and include the following; web and application User interface, system, tools, documentation, training, service desk.
LANG-02	The ***LSRMS Solution*** tools and applications should provide all Users with the ability to set a preferred default language for their use, if the User has not indicated a preference.

SOW NUM	Requirement (RATED)
LANG-03	Should support Canadian English and Canadian French
LANG-04	The following ***LSRMS Solution*** User interface elements should be available in both Canada's Official Languages; a) Input Controls: checkboxes, radio buttons, dropdown lists, list boxes, buttons, toggles, text fields, date field, text terminal window, b) Navigational Components: breadcrumb, slider, search field, pagination, slider, tags, icons, tabs, c) Informational Components: tooltips, icons, progress bar, notifications, message boxes or windows, dialog box, modal windows (pop up), d) Menus: menu bar, menu, context menu, extra menus, primary and secondary menus, ~~e)~~ Browser: Microsoft Internet Explorer 11, Edge (and two previous versions), and f) Landing page, homepage, welcome or login page.
LANG-05	When using the ***LSRMS Solution*** tools and applications the User should be able to toggle between either Canada's Official Languages.

SOW NUM	Requirement (RATED)
LANG-06	The ***LSRMS Solution*** tools and applications should allow certain input control fields to be entered in both Canada's Official Languages, regardless of the individual User's language of choice.
LANG-07	The ***LSRMS Solution*** tools and applications should be capable of integrating both Canada's official language information in its database(s).
LANG-08	Reports generated from the ***LSRMS Solution***, by Users and resource(s) should be available in both Canada's Official Languages.
LANG-09	The ***LSRMS Solution*** should support display, search and capture of the ISO 8859-1 character set (specifically Canadian French characters).
LANG-10	The ***LSRMS Solution*** should support a Canadian bilingual keyboard.

3.4 Section C – Portal Requirements

3.4.1 Objective

The ***LSRMS Solution*** must service internal Translation Bureau resource(s)~~,~~ external resource(s) and GC departments and agencies (TB clients). It should provide of the box templates that can be used and modified to allow TB clients, (internal~~,~~ and external resource(s) based on their role, access rights and permission), secure access to information, ***LSRMS Solution*** features and functionalities, and tools for Translation, Terminology, and Interpretation.

The portal functionalities are to establish a secure, reliable and accessible environment for all internal Translation Bureau resource(s), external ***Suppliers***/ LPSs, GC departments and agencies (TB clients) as outlined within the various sections of the Statement of Work.

3.4.2 Requirements

SOW NUM	Requirement (MANDATORY)
PRTL-CLNT-01	The ***LSRMS Solution*** must have a secure, web-based, customizable TB client portal.

SOW NUM	Requirement (RATED)
General The ***LSRMS Solution*** should provide the following functionalities;	
PRTL-GEN-02.1	For a User with the proper role, access rights, and permission to be able to create, edit, delete, view, and publish content in the portal.
PRTL-GEN-02.2	For a User with the proper role, access rights, and permission to view current and expired system notices in the portal.
PRTL-GEN-02.3	For a User with the proper role, access rights, and permission should be able to create and configure popup notifications for TB client account and information updates, internal Translation Bureau resource(s), and external resource(s) profile and information updates.
PRTL-LANG-03	The ***LSRMS Solution*** should deliver a comprehensive portal interface for all Users (internal and external) of the solution that includes information, training, support, and present all Users with at-a-glance information that is relevant to their roles and responsibilities.

SOW NUM	Requirement (RATED)
PRTL-CONT-04	**Content and Data** The ***LSRMS Solution*** should allow User with the appropriate role, access rights and permission to create, edit, delete, review, approve and publish content in the Portal.
PRTL-LAND-05	**Landing Page** The LSRMS should allow for the creation and configuration of specific page(s) on a web site for the TB client that includes; a) Registration to generate a User profile, b) Deliver relevant communications, c) Provide information on what is available through the LSRMS; and d) Enable One-Time Login for GC User and have authenticated access to all components of the LSRMS based on User with the appropriate role, access rights and permission.
PRTL-DASH-06	**Dashboards** The LSRMS should provide access to dashboards with the following functionalities and information: a) Set goals and expectations for specific individual User or groups, b) Highlight exceptions and provide alerts when problems occur, c) Communicate progress and success, d) Provide a common interface for interacting with and analyzing business data, e) For a User with the proper role, access rights, and permission to configure and utilize various reusable templates with different features and controls including the ability to select from a variety of configurable dashboards, f) For User with the proper role, access rights, and permission to organize their dashboard; and g) For User with the proper role, access rights, and permission to view, search and organize (e.g. Sort and filter) their work activities.
Login The ***LSRMS Solution*** should provide the following functionalities;	
PRTL-LOGN-07.1	To provide secure login access for TB clients, internal, external resource(s) based on GC IT Security Standards and security control profiles.
PRTL-LOGN-07.2	To configure and enable one-time login, for GC resource(s), and provide based on role, access rights, and permission controlled access to the features, functionalities, and tools of the ***LSRMS Solution***.
PRTL-LOGN-07.3	For a User with the proper role, access rights, and permission to configure and manage; login, self-serve features, TB client, internal, and external resource(s) registration, help section User guide, frequently asked questions (FAQ), and any form of online training.
PRTL-LOGN-07.4	To configure the terms of use of LSRMS in the order that it appears at various predefined stages of the process to confirm User acceptance of the LSRMS (configurable re-occurrence).
Communication The ***LSRMS Solution*** should provide the functionalities:	
PRTL-COMM-08.1	To enable and facilitate the communication between internal, external resource(s) , GC departments and agencies (TB clients),
PRTL-COMM-08.2	For User to access all electronic communications within LSRMS between internal, external ***Suppliers***/ LSPs, GC departments and agencies.

SOW NUM	**Requirement (RATED)**
PRTL-COMM-08.3	To configure notification message and distribute as per established workflow LSRMS for example approval of requests, status of invoice, credit memo.
PRTL-COMM-08.4	To notify User when TB client has acknowledged their requests for example request for quote), orders (requests), and messages within LSRMS.
PRTL-COMM-08.5	For a User with the proper role, access rights, and permission to create and distribute electronic, outward communication to portal User.
PRTL-COMM-08.6	To communicate to all User or a subset of User for example, being able to create e-mail distribution lists).
TB Client The ***LSRMS Solution*** should provide the following functionalities:	
PRTL-CLNT-09.1	To submit service requests online.
PRTL-CLNT-09.2	To view the service requests progress online in real time throughout the workflow.
PRTL-CLNT-09.3	Notify when the service request completion date has been changed.
PRTL-CLNT-09.4	To search, filter, view, download, print and save past and current service requests.
PRTL-CLNT-09.5	To search, filter, view, download, print and save past and current quote for work to be performed.
PRTL-CLNT-09.6	To search, filter, view, download, print and save past and current service request invoicing.
PRTL-CLNT-09.7	To add comments to active service requests submitted online in The ***LSRMS Solution*** throughout the workflow.
PRTL-CLNT-09.8	To communicate with Bureau resource(s) on active service requests submitted online in the ***LSRMS Solution*** throughout the workflow.
PRTL-CLNT-09.9	To configure parameters to generate reports past and current on but not limited to; service requests, quotes, and invoices.
PRTL-CLNT-09.10	Upload reference material.
PRTL-CLNT-09.11	Create service requests and upload Protected A and B documents.
PRTL-CLNT-09.12	Create service requests for all information classification categories.
PRTL-CLNT-09.12.1	Restrict uploading of any documents classified greater than Protected B.
PRTL-CLNT-09.13	Should be able to restrict access to features and functionalities based on role, access rights, and permission.
Internal Translation Bureau resource(s) The ***LSRMS Solution*** should provide the following functionalities:	
PRTL-INTRES-10.1	To communicate with Bureau resource(s) on active requests (***project***) submitted online in the ***LSRMS Solution*** throughout the workflow.
PRTL-INTRES-10.2	To retrieve the translation package for example, source text, and reference material.
PRTL-INTRES-10.3	View and display progress of their Task(s) and activities on all active requests (***project***).
PRTL-INTRES-10.4	Search, filters and generate reports on requests (***project***) for example active, cancelled, delivered, and inactive Tasks.
PRTL-INTRES-10.5	Upload translated documents and reference material.
PRTL-INTRES-10.6	View their workload in real time.
PRTL-INTRES-10.7	View their workload in real time on mobile device.
PRTL-INTRES-10.8	Search, filter, view, download, print and save calendar and time table.

SOW NUM	Requirement (RATED)
External resource(s) The ***LSRMS Solution*** should provide the following functionalities:	
PRTL-EXTRES-11.1	To communicate with Bureau resource(s) on active requests (***project***) submitted online in The ***LSRMS Solution*** throughout the workflow.
PRTL-EXTRES-11.2	View and display progress of their Task(s) and activities on all active requests (***project***).
PRTL-EXTRES-11.3	Search, filters and generate reports on requests (***project***) for example active, cancelled, delivered, and inactive Tasks.
PRTL-EXTRES-11.4	Search, filter, view, download, print and save past and current service request invoicing,
PRTL-EXTRES-11.5	Upload translated documents and reference material.
PRTL-EXTRES-11.6	Should be able to enter their actual time per Task for Translation, Terminology and Interpretation.
PRTL-EXTRES-11.7	View their workload in real time.
PRTL-EXTRES-11.8	Search, filter, view, download, print and save past and current evaluation score.
PRTL-EXTRES-11.9	Search, filter, view, download, print and save calendar and time table.
PRTL-EXTRES-11.10	Should allow the access to external resource(s) to retrieve the work and return the reference material, translated text and documents.

3.5 SECTION D - WORKFLOW MANAGEMENT

3.5.1 Objective

The ***LSRMS Solution*** must allow the capability to configure Tasks and activities as part of the workflow that may require manual intervention, be Semi-automated and Fully Automated, in order to manage the entire end-to-end process flows and Bureau services for Translation, Terminology, and Interpretation. It must cover the submission of a ***project*** (request), delivery of the service, and invoicing.

3.5.2 Requirements

SOW NUM	Requirement (MANDATORY)
WF-01	The Contractor must deliver a solution that provides the mechanism to build, configure, and tailor the workflows

SOW NUM	Requirement (RATED)
The ***LSRMS Solution*** should provide the following functionalities:	
WF-02	To provide error information to User during the creation of the workflow for example error messages for logic errors in workflow creation and to provide information to the User as to why a workflow cannot proceed.
WF-03	To create, edit, delete, configure and test workflows which includes manual, Semi-automated and Fully Automated workflows.

SOW NUM	Requirement (RATED)
WF-04	For a User with the proper role, access rights and permission to be able to; a) Create, add, edit and delete ***project*** Tasks and activities in a *manual, Semi-automated and Fully Automated* workflow whether it is sequential or parallel, b) Tailor, configure and manage ***project*** Tasks and activities in a manual, Semi-automated, and Fully Automated workflow whether it is sequential or parallel, c) Add additional ***project*** Tasks and activities to specific workflow instances, at any interval whether the flow is sequential or parallel for example; to support functions, document quality evaluations, and d) Set business and validation rules for manual, Semi-automated and Fully Automated workflows.
WF-05	For a User with the proper role, access rights and permission to be able to configure; a) End to end workflow from TB client ***project*** (request) submission, delivery and invoicing, b) Workflow approval process, c) Workflow statuses, d) Workflow notifications, e) Who it is assigned to (group or individual), f) The action required (watcher only, approve/deny or edit/approve/deny), g) List of acceptable reasons for approving or denying, and h) Escalation rules (length of time dormant, group or individual to escalate to).
WF-06	Manage ***project*** deadlines.
WF-07	View the status of the ***project*** Task in the workflow in real time.
WF-08	Add, edit and delete comments to the ***project*** as a whole and to ***project*** Tasks in the workflow.
WF-09	To retain the history of all ***project*** and ***project*** Task comments added, edited and deleted with a User ID and times stamp.
WF-10	Allow a User with the proper role, access rights, and permission to configure a time frame for the execution of a Task and *activity*.
WF-11	Allow tracking the reception, processing of Tasks and activities related to the required support.
WF-12	Provide the capability to automate the preparation of' a kit to the external resource(s) comprised of other documents to be translated, relevant extracts from the TM, the analysis report, and reference documentation.

3.6 SECTION E – WORKLOAD MANAGEMENT

3.6.1 Objectives

The ***LSRMS Solution*** must include a workload management component that can be used to manage internal Translation Bureau and external resource(s) for Translation, Terminology, Interpretation and the support thereof, which may include proofreading, desktop publishing and documentation services. It will provide the visibility to more effectively plan, organize, schedule, and distribute the workload to resource(s) either manually or automatically.

3.6.2 Requirements

SOW NUM	Requirement (MANDATORY)
WL-MAN-01	The ***LSRMS Solution*** must have workload management functionality.
WL-MAN-02	The ***LSRMS Solution*** must allow a User with the proper role, access rights and permission to configure the collective agreement parameters and coefficients used to calculate the total number of hours worked by an interpreter refer to *Part 12 Appendix E - Interpretation Workload Calculation and Example*.

SOW NUM	Requirement (RATED)
WL-03	The ***LSRMS Solution*** should include the following workload scheduling capability to; web-based interface, be able to display and view one or many resource(s) schedules based on a User with the proper roles, access rights, and permission, and be able to interact with the schedule.
WL-04	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to define and configure the workload schedule business rules, validation, and priorities.
WL-05	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to add, edit, and delete a workload schedule.
WL-06	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to schedule the following; a) Tasks, b) Events, c) Local and remote resource(s) across different time zones, d) Catering, e) Equipment, f) Meeting rooms, and g) Assign workstations.
WL-07	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to select or enter, and track the type of absence in the workload schedule and include the following; a) Training, b) Leave (sick, compassionate, maternity and parental), c) Full and part time assignments, d) Time off / appointment, e) Holidays, f) Vacation, g) Gradual return, and h) Overtime.
WL-08	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to distribute the latest workload schedule.
WL-09	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to set and configure workload schedule.
WL-10	The ***LSRMS Solution*** should allow the distribution of the workload schedule to be sent manually and automatically at a configurable time.
WL-11	The ***LSRMS Solution*** should track changes to the workload schedule with a User name or ID, time stamp, and description.

SOW NUM	Requirement (RATED)
WL-12	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to add optional comments to Tasks.
WL-13	The ***LSRMS Solution*** should retain the Task comment history with a User name or ID, and time stamp.
WL-14	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to add links to reference documents to a Task.
WL-15	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to update a workload schedule in real time.
WL-16	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to view a single resource(s) workload schedule or multiple.
WL-17	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to print a workload schedule of a single resource(s) or multiple.
WL-18	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to search and filter resource(s) by; a) Availability, b) Skills, c) Domain specialization, d) Language, e) Security clearance, f) TB client, g) Internal Translation Bureau or external LSP resource(s) , h) Contract, and i) Location.
WL-19	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to save searches and filters for later use.
WL-20	The ***LSRMS Solution*** should allow resource(s) to log in to view one or many workload schedule based on a User with the proper role, access rights, and permission.
WL-21	The ***LSRMS Solution*** should allow a single resource(s) with the proper role, access rights, and permission to enter, edit, delete, and view their time and expenses.
WL-22	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to enter time in bulk for example; to vacation, and training.
WL-23	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to enter, edit, delete, view, and approve time and expenses (any and all expenses).
WL-24	The ***LSRMS Solution*** should be able to track ***project*** or TB client hours and compare billable versus non-billable ***project*** hours or ***project*** word count.
WL-25	The ***LSRMS Solution*** should be able to compare resource(s) scheduled time versus reported actual time.
WL-26	The ***LSRMS Solution*** should allow a User with the proper roles, access rights, and permission to set the date range for pre-defined and custom workload schedule reports.

SOW NUM	Requirement (RATED)
WL-27	The ***LSRMS Solution*** should allow the definition and configuration of automated alerts and warning notifications for: a) Certification, contract and rate expiry dates, b) resource(s) allocation conflicts, c) Approaching deadlines and budget thresholds, d) Potential under- or over-utilization of resource(s).
WL-28	The ***LSRMS Solution*** should allow a User with the proper roles, access rights, and permission to set up reminders.
WL-29	The ***LSRMS Solution*** should provide APIs (Application Programming Interface) for 3rd party calendar applications.
WL-30	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to restrict views, and access to features and functionalities.
WL-31	The ***LSRMS Solution*** should provide visual status indicators for: a) Task progress, b) resource(s) utilization, c) Availability.
WL-32	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to set up and configure for scheduling, the resource(s) working Canadian time zone.
WL-33	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to schedule resource(s) in all Canadian time zones.
WL-34	The ***LSRMS Solution*** should indicate to a User with the proper role, access rights and permission that a resource(s) is in a different Canadian time zone.
WL-35	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to add, edit and delete TB client profile that contains; account, contact information, TB client approved lexicons, preferences, style guides, reference material, approver contact, method of communication and/or correspondence for example email, phone, special instructions (common, most often requested).
WL-36	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to add, edit and delete internal Translation Bureau resource(s) profile that contains; role, qualification, certification, language, security clearance, Canadian time zone, translation domains and specialties (aviation terminology, medical).
WL-37	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to add, edit and delete external Resource(s) profile that contains; area of expertise by domain(s), contract information, number of contracts, contact information, skillset, specialization, security clearance level, working language(s) (Interpretation), evaluation score, resource(s) calendar and time table, number of residual words remaining on the contract (and rates).
WL-38	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to add, edit and delete the word scale used to calculate the hours planned for invoicing and the hours planned for execution based on the service requested by the TB client for example; Translation 214 words/hour, and Revision 856 words/hour.

SOW NUM	Requirement (RATED)
WL-39	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to add, edit and delete the TB client billing rate used to calculate the invoice for the work performed.
WL-40	The ***LSRMS Solution*** should allow real-time monitoring of the daily capacity of the external translation resource(s) and the number of words/hours remaining in the contract.
WL-41	The ***LSRMS Solution*** should be able to generate a document manually and automatically containing the information necessary for the award of the work to an external resource(s) for example, Task authorization.

3.7 SECTION F – COMPUTER AIDED TRANSLATION (CAT)

3.7.1 Objectives

Computer Aided Translation (CAT) is a key component of the Translation Bureau (TB), is essential to its efficient success, and is used to fulfil and expedite the delivery process of a translation request which generally consists of: TB client request, source file preparation, analysis and pre-processing, translation, including support functions such as proofreading and spell-checking, verification checks, delivery to the TB client, and TB client billing. Many of the CAT Contractor s come with an array of tools such as, Analyzer, Editor, Translation Memory (TM), Alignment, Concordancer, Machine Translation (MT), TermBase, Term Extractors, Quality Assurance, and Localization tools. In addition, some Contractor s include ***project*** (request) management, Content Management Systems (CMS), application programming interfaces (API) that allow connection to 3rd party tools, workflow, and workload management tools. All the tools combined provide a comprehensive suite that can take the Translation Bureau to the next level.

3.7.2 Overview

3.7.2.1 Analyzer

The analyzer is a tool used to estimate the work effort required by a Translator to translate a document and to provide a TB client with an estimate on the cost to translate a document. The analyzer performs a word breakdown analysis on the document to be translated by comparing it against a Translation Memory (TM) and Corpora. It provides the following:

a) Total word counts,
b) Exact match (100%) which displays the number and/or percentage of words, characters or segments for which a 100% match was found,
c) Fuzzy match which display the number and/or percentage of words, characters or segments that were translated with a less than perfect (100%) match (the degree of match is indicated by the percentage figure),
d) Repetitions which displays the number and/or percentage of words, characters or segments that are repetitions of previously counted words,
e) Context match which displays the number and/or percentage of words, characters or segments for which a context match was found.

3.7.2.2 Editor

The editor is the CAT tool frontend that translators use to open a source file for translation, and query the memory and terminology databases for relevant data. It is also the workspace in which translators can use to write their own translations if no matches are found, and the interface for sending finished sentence (segments) pairs to the translation memory and terminology pairs to the term base.

3.7.2.3 Translation Memory (TM)

A translation memory or TM is a database that contains past translations, aligned and ready for reuse in matching pairs of source and target segment, and is normally demarcated by explicit punctuation − it is therefore commonly a sentence, but can also be a title, caption, or the content of a table cell. A typical TM entry, consists of a source segment linked to its translation, plus relevant metadata (e.g. time/date and author stamp, TB client name, subject matter, etc.). The TM application also contains the algorithm for retrieving a matching translation if the same or a similar segment arises in a new text. The majority of the ***commercially available solutions*** can import and export memories using Translation Memory eXchange (TMX) format, an open XML standard created by OSCAR (Open Standards for Container/Content Allowing Re-use), a special interest group of LISA (Localization Industry Standards Association).

3.7.2.4 Alignment

Alignment is a way of making use of previous translations, it converts previously translated documents into translation segments so that they can be added to a translation memory (TM). The alignment tool matches the source and target language files side-by-side, to determine which pairs belong together. Once, the process is done it is sent for verification to ensure each segment, and their respective matches are correct and fixing (or deleting where necessary) those that are incorrect. Alignment tools implement some editing and monitoring functions so that segments can be split or merged as required, and extra or incomplete segments can be detected, to ensure a perfect 1:1 mapping between the two documents. The LISA/OSCAR Segmentation Rules eXchange (SRX) open standard was created to optimize performance across systems.

3.7.2.5 Concordancer

Concordancing is a means of accessing a corpus of text to show how any given word or phrase in the text is used in the immediate contexts in which it appears. Concordances are frequently used in linguistics, when studying a text. A typical concordancer would allow a person to enter a word or phrase and search for multiple examples of how that word or phrase is used in everyday speech or writing.

3.7.2.6 Machine Translation (MT)

Machine translation (MT) is automated translation or translation carried out by a computer. It is a process, sometimes referred to as Natural Language Processing which uses a bilingual data set and other language assets to build language and phrase models used to translate text. The output of the translation is often a rough translation that is often incorrect and ungrammatical which usually requires post-editing by a person but is cheaper/faster to fix than to translate from scratch. MT can also be used interactively, while a linguist is translating text in a CAT tool the MT will offer suggestions.

3.7.2.7 TermBase

The TermBase is similar to the TM of reusable segments memory, but instead functions at term level by managing searchable/ retrievable glossaries containing specific pairings of source and target terms plus associated metadata. The TermBase monitors the active translation segment in the editor against a database such as, a bilingual glossary and when it detects a source term match, it will prompt with the corresponding target equivalent. There can be a variety of glossaries in a TermBase that are segregated for different criteria example domains, specialization, TB clients and ***projects.*** To facilitate and enhance the exchange capability, a Terminology

Base eXchange (TBX) open standard was eventually created by OSCAR/LISA. Nowadays most sophisticated systems are TBX compliant.

3.7.2.8 Term Extraction

The goal of terminology extraction is to automatically extract relevant terms from a given corpus. Terms can be extracted either manually, or by highlighting words in documents and transferring them to a program, such as Word or Excel, or automatically, by using term extraction tools. The Standard that defines an XML-based framework for representing structured terminological data referred to as TermBase eXchange (TBX).

3.7.2.9 Quality Assurance (QA)

QA modules perform linguistic controls by checking terminology usage, spelling and grammar, and confirming that any non-translatable items (e.g. certain proper nouns) are left unaltered. They can also detect if numbers, measurements and currency are correctly rendered according to target language conventions. At the engineering level, they ensure that no target segment is left untranslated, and that the target format tags match the source tags in both type and quantity. With QA checklist conditions met, the document can be confidently exported back to its native format for final proofing and distribution.

3.7.2.10 Requirements

SOW NUM	Requirement (MANDATORY)
CAT-MAN-01	The ***LSRMS Solution*** must have a suite of CAT tools that includes analyzer, editor, translation memory, TermBase, machine translation and quality assurance modules.

SOW NUM	Requirement (RATED)
General (System = CAT tools) The following capabilities should be provided;	
CAT-GEN-02.1	The ***LSRMS Solution*** should be accessible online and offline.
CAT-GEN-02.2	The ***LSRMS Solution*** should be available in both official languages English and French.
CAT-GEN-02.3	The ***LSRMS Solution*** should allow a User to add, edit and delete comments.
CAT-GEN-02.4	The ***LSRMS Solution*** should retain the history of all the comments added, edited and deleted with a User ID and times stamp.
CAT-GEN-02.5	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to restrict access to features and functionalities.
CAT-GEN-02.6	The ***LSRMS Solution*** should include multiple languages.
CAT-GEN-02.7	The ***LSRMS Solution*** should provide a predefined and customizable metadata list.
CAT-GEN-02.8	The ***LSRMS Solution*** should provide customizable search functions.
CAT-GEN-02.9	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to review an incoming document in order to establish the effort and cost of translating it and include the following: a) Cleaning, b) Pre-translation, c) Word counts, d) Terminology translation, e) Text package creation, and f) Optical Character Recognition (OCR) (PDF format).

SOW NUM	Requirement (RATED)
Analyzer The following analyzer capabilities should be provided;	
CAT-ANLZ-03.1	The ***LSRMS Solution*** should allow documents to be uploaded manually.
CAT-ANLZ-03.2	The ***LSRMS Solution*** should allow documents to be uploaded automatically.
CAT-ANLZ-03.3	The ***LSRMS Solution*** should allow the following format types to be processed: a) MS Word (doc.docx), b) MS Excel (xls, xlsx), c) MS Power Point (ppt, pptx), d) PDF, and e) MS Visio (vsd).
CAT-ANLZ-03.4	The ***LSRMS Solution*** should allow documents to be scanned.
CAT-ANLZ-03.5	The ***LSRMS Solution*** should allow the following documents types to be converted; a) MS Word (doc, docx), b) Txt, c) Odt, and d) Wpd.
The ***LSRMS Solution*** should provide an analysis report based on segments.	
CAT-ANLZ-03.6.1	Analysis report information should contain: a) File name with file extension, b) Word count – number redundant, number new, total, c) Segment count - number redundant, number new, total, d) ***Project*** name or number, and e) Number of files
CAT-ANLZ-03.6.2	Word distribution analysis details should contain; a) Exact – number of words, weight in percent, b) Fuzzy - number of words, weight in percent, c) Repetition - number of words, weight in percent, and d) New - number of words, weight in percent
CAT-ANLZ-03.7	The ***LSRMS Solution*** should allow fuzzy matches to be configurable.
CAT-ANLZ-03.8	The ***LSRMS Solution*** should allow the following MS Word elements to be included in the analyzer word count; a) Revision marks (Track Changes), b) Text boxes including sidebars, c) Tables of contents (with field codes and manual), d) Headers and footers, e) Footnotes, f) Endnotes, g) References, h) Tables, and i) Graphs made with publishing software.
CAT-ANLZ-03.9	The ***LSRMS Solution*** should allow the following MS Power Point elements to be included in the analyzer word count; a) Notes pages, b) Slide masters, c) Graphs made and saved with publishing software, d) Headers and footers,

SOW NUM	**Requirement (RATED)**
	e) Text Box, and f) Tables.
CAT-ANLZ-03.10	The ***LSRMS Solution*** should allow the following MS Excel elements to be included in the analyzer word count; a) Multiple tabs, b) Name given to the tab, c) Hidden content (cells, columns, lines, Tabs), d) Comments, e) Revision marks, f) Hidden text, g) Text boxes, h) Drop-down menus, and i) Tables
CAT-ANLZ-03.11	The ***LSRMS Solution*** should allow the following MS Visio elements to be included in the analyzer word count; Multiple tabs.
CAT-ANLZ-03.12	The ***LSRMS Solution*** should allow the following Adobe PDF elements to be included in the analyzer word count; Text format (editable).
CAT-ANLZ-03.13	The ***LSRMS Solution*** should display the content of the file to be translated, divided into segments.
CAT-ANLZ-03.14	The ***LSRMS Solution*** should display the source and target language.
CAT-ANLZ-03.15	The ***LSRMS Solution*** should display a numbered list of the source segments.
CAT-ANLZ-03.16	The ***LSRMS Solution*** should display the source segments and target segments equivalent side by side.
CAT-ANLZ-03.17	The ***LSRMS Solution*** should indicate the source segment status such as: i. Exact ii. Fuzzy iii. Repetition iv. New
CAT-ANLZ-03.18	The ***LSRMS Solution*** should indicate the target segment equivalent match percentage.
CAT-ANLZ-03.19	The ***LSRMS Solution*** should allow the analysis report to be saved.
CAT-ANLZ-03.20	The ***LSRMS Solution*** should allow the analysis report to be printed.
CAT-ANLZ-03.21	The ***LSRMS Solution*** should display error messages if analysis report cannot be executed.
CAT-ANLZ-03.22	The ***LSRMS Solution*** should display error messages if analysis report not complete.
CAT-ANLZ-03.23	The ***LSRMS Solution*** should provide an indication if the document is uploaded manually or automatically is password protected.
CAT-ANLZ-03.24	The ***LSRMS Solution*** should allow word count rules to be configurable for; a) Character type, b) Numbers, and c) Symbols.
CAT-ANLZ-03.25	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to set the parameters for estimating the number of hours of work effort, required for the translation based on the weighted word count.
CAT-ANLZ-03.26	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to set the parameters to estimate the cost of a TB client request for translation, based on the weighted word count and rate.

SOW NUM	**Requirement (RATED)**
CAT-ANLZ-03.27	The ***LSRMS Solution*** should allow the analysis report to be exported to; a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) XML, and e) CSV.
CAT-ANLZ-03.28	The ***LSRMS Solution*** should allow the analysis report to be displayed in a browser.
CAT-ANLZ-03.29	The ***LSRMS Solution*** should detect source language.
CAT-ANLZ-03.30	The ***LSRMS Solution*** should detect images
Editor The following editor functionality should be provided;	
CAT-EDIT-04.1	The ***LSRMS Solution*** must be accessible online and offline.
CAT-EDIT-04.2	The ***LSRMS Solution*** should have configurable User interface.
CAT-EDIT-04.3	The ***LSRMS Solution*** should allow the conversion of the HTML (HyperText Markup Language) web page to a word document for offline work.
CAT-EDIT-04.4	The ***LSRMS Solution*** must be able to translate multiple document format types.
CAT-EDIT-04.5	The ***LSRMS Solution*** should allow a User to select how source and target segments are displayed.
CAT-EDIT-04.6	The ***LSRMS Solution*** should have the capability to; a) Search & Replace, b) Delete, c) Undo Changes, d) Sort, e) Merge, f) Tag management, g) Advanced highlighting, and h) Auto-suggest.
CAT-EDIT-04.7	The ***LSRMS Solution*** must allow a User with the proper role, access rights and permission to restrict access to features and functionalities.
CAT-EDIT-04.8	The ***LSRMS Solution*** should allow translating multiple documents at one time.
CAT-EDIT-04.9	The ***LSRMS Solution*** should allow what you see is what you get (WYSIWYG).
CAT-EDIT-04.10	The ***LSRMS Solution*** should allow rich text editing.
CAT-EDIT-04.11	The ***LSRMS Solution*** should allow source and target context comparison.
CAT-EDIT-04.12	The ***LSRMS Solution*** should provide APIs (Application Programming Interface) for 3rd party editors.
CAT-EDIT-04.13	The ***LSRMS Solution*** should allow a User to add, edit and delete comments to the segments.
CAT-EDIT-04.14	The ***LSRMS Solution*** should retain the history of all comments added, edited and deleted with a User name or ID and times stamp.
CAT-EDIT-04.15	The ***LSRMS Solution*** should allow User to customize the editor searches using regular expressions.
CAT-EDIT-04.16	The ***LSRMS Solution*** should provide connectors to 3rd party editing tools.
CAT-EDIT-04.17	The ***LSRMS Solution*** should allow voice recognition software to be used.
CAT-EDIT-04.18	The ***LSRMS Solution*** should have quick document translation functionality using Contractor or 3rd party machine translation or translation memories.
CAT-EDIT-04.19	The ***LSRMS Solution*** should have concordancer functionality.

SOW NUM	**Requirement (RATED)**
CAT-EDIT-04.20	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to configure keyboard short cuts for features and functionalities.
Translation Memory (TM) The following Translation Memory functionality should be provided;	
CAT-TM-05.1	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to create, edit and delete TM.
CAT-TM-05.2	The ***LSRMS Solution*** should allow import/export of TM content.
CAT-TM-05.3	The ***LSRMS Solution*** should comply with XLIFF 2.0 (XML Localisation Interchange File format).
CAT-TM-05.4	The ***LSRMS Solution*** should comply with TMX 1.4B (Translation Memory Exchange format).
CAT-TM-05.5	The ***LSRMS Solution*** should allow real time updating of TM.
CAT-TM-05.6	The ***LSRMS Solution*** should allow simultaneous searches through multiple TMs.
CAT-TM-05.7	The ***LSRMS Solution*** should have the capability to; a) Search & Replace, b) Delete, c) Undo Changes, d) Sort, e) Merge, f) Auto-suggest, and g) Duplicate Removal from TM.
CAT-TM-05.8	The ***LSRMS Solution*** should comply with UTF-8 and UTF-16 (Unicode Transformation Format).
CAT-TM-05.9	The ***LSRMS Solution*** should allow the creation of virtual TM by combining existing TMs.
CAT-TM-05.10	The ***LSRMS Solution*** should also allow Users with the appropriate roles, access rights and permission to manually correct misaligned segments using, for example; merge, swap, insertion and deletion functions.
CAT-TM-05.11	The ***LSRMS Solution*** should have TM management functionalities.
CAT-TM-05.12	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to restrict access to features and functionalities.
CAT-TM-05.13	The ***LSRMS Solution*** should allow manual and automatic storage of the original source, updated source, and final target documents to TB client such as references and ***Suppliers*** references.
CAT-TM-05.14	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to configure the storage retention period for original source, updated source, and final target documents.
CAT-TM-05.15	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to create, edit, and delete tags and metadata for the original source, updated source and final target documents.
CAT-TM-05.16	The ***LSRMS Solution*** should support alphanumeric naming and numbering of stored files and documents.
CAT-TM-05.17	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to create, edit, and delete different types of TMs for example; a) ***Project***, b) Public,

SOW NUM	Requirement (RATED)
	c) Private, d) Personal, and e) TB client.
CAT-TM-05.18	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to configure the retention period for TMs.
CAT-TM-05.19	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to configure parameters for manual and automatic purging.
CAT-TM-05.20	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to create, edit, and delete tags and metadata for TM.
CAT-TM-05.21	The ***LSRMS Solution*** should support alphanumeric naming and numbering of TMs.
CAT-TM-05.22	The ***LSRMS Solution*** should allow manual and automatic conversion of original source, updated source, and final target documents into text.
CAT-TM-05.23	The ***LSRMS Solution*** should allow manual and automatic batch conversion of original source, updated source, and final target documents into text.
CAT-TM-05.24	The ***LSRMS Solution*** should notify a User with the proper role, access rights and permission of any errors or failures on single or batch conversion of original source, updated source, and final target documents into text.
CAT-TM-05.25	The ***LSRMS Solution*** should log any errors or failures with a description and time stamp on single or batch conversion of original source, updated source, and final target documents into text.
CAT-TM-05.26	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to generate reports on any errors or failures on single or batch conversion of original source, updated source, and final target documents into text.
CAT-TM-05.27	The ***LSRMS Solution*** should allow the original source, updated source and final target text to be manually and automatically segmented, paired, aligned and stored.
CAT-TM-05.28	The ***LSRMS Solution*** should notify a User with the proper role, access rights and permission of any errors or failures on text segmentation, pairing, aligning and storing.
CAT-TM-05.29	The ***LSRMS Solution*** should log any errors or failures with a description and time stamp on text segmentation, pairing, aligning and storing.
CAT-TM-05.30	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to generate reports on any errors or failures on text segmentation, pairing, aligning and storing.
CAT-TM-05.31	The ***LSRMS Solution*** should allow manual and automatic storage of the original source, updated source, and final target documents.
CAT-TM-05.32	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to configure the storage retention period for original source, updated source, and final target documents.
CAT-TM-05.33	The ***LSRMS Solution*** should allow concurrent access to the same translation memory by multiple Users (893 translators) translating parts of the same document or closely related documents.
CAT-TM-05.34	The ***LSRMS Solution*** should be able to import a bilingual TMX file into a TM with both source-target or target-source language settings for example, the software should be able to import

SOW NUM	Requirement (RATED)
	a TMX file including both English and French segments into a English-French and into a French-English TM.
CAT-TM-05.35	The ***LSRMS Solution*** should be able to import a multilingual TMX file into a bilingual TM with any of the relevant language pairs as language settings for example, the software should be able to import a TMX file including Canadian English and Canadian French segments into an Canadian English-French and into a Canadian French-English TM.
Machine Translation (MT) The following MT functionality should be provided;	
CAT-MT-06.1	The ***LSRMS Solution*** should provide APIs (Application Programming Interface) for 3rd party machine translation tools.
TermBase The following TermBase functionality should be provided;	
CAT-TRMB-07.1	The ***LSRMS Solution*** should allow User to customize TermBase searches using regular expressions.
CAT-TRMB-07.2	The ***LSRMS Solution*** should have the capability to; a) Search & Replace, b) Delete, c) Undo Changes, d) Sort, e) Merge, f) Auto-suggest, g) Duplicate Removal from TermBases.
CAT-TRMB-07.3	The ***LSRMS Solution*** should allow multilingual terminology management.
CAT-TRMB-07.4	The ***LSRMS Solution*** should allow bilingual term extraction.
CAT-TRMB-07.5	The ***LSRMS Solution*** should have auto-term extraction.
CAT-TRMB-07.6	The ***LSRMS Solution*** should allow simultaneous searches through multiple term databases.
CAT-TRMB-07.7	The ***LSRMS Solution*** should allow verification of term against predefined set of terms.
CAT-TRMB-07.8	The ***LSRMS Solution*** should allow remote and offline synchronized term bases per ***project***,
CAT-TRMB-07.9	The ***LSRMS Solution*** should allow importing and exporting various TermBase types such as terminology, dictionaries, glossaries, lexicons in different formats; a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) XML, and e) CSV.
CAT-TRMB-07.10	The ***LSRMS Solution*** should provide APIs (Application Programming Interface) for 3rd party TermBases.
Quality Assurance (QA) The following quality assurance functionality should be provided;	
CAT-QA-08.1	The ***LSRMS Solution*** should provide checks for; a) Inconsistencies in numbers, b) Missing terminology, c) Spelling errors, d) Grammar, e) Incomplete translations,

SOW NUM	Requirement (RATED)
	f) Empty translations, g) Repeated words, h) Double spaces, i) Punctuation, j) Capitalization, k) Terminology against predefined set of terms, l) Segment by segment, and m) Tag management and tag validation.
CAT-QA-08.2	The ***LSRMS Solution*** should provide notifications for work submitted with unresolved errors.
CAT-QA-08.3	The ***LSRMS Solution*** should allow User with the proper role, access rights and permission to customize QA checks using regular expressions.
CAT-QA-08.4	The ***LSRMS Solution*** should allow real-time on-the-fly QA checks based on predefined or customizable configuration.
CAT-QA-08.5	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to enable and disable QA ***project*** Tasks.
CAT-QA-08.6	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to generate the following QA report types; a) Pre-defined, b) Customizable, c) Issues, and d) Summary.
CAT-QA-08.7	The ***LSRMS Solution*** should allow the QA report to be saved.
CAT-QA-08.8	The ***LSRMS Solution*** should allow the QA report to be printed.
CAT-QA-08.9	The ***LSRMS Solution*** should allow the QA report to be exported in; a) MS Excel (xls, xslx), b) MS Word (doc, docx), c) PDF, d) XML, and e) CSV.
CAT-QA-08.10	The ***LSRMS Solution*** should provide APIs (Application Programming Interface) for 3rd party QA tools.
CAT-QA-08.11	The ***LSRMS Solution*** should comply with: a) LISA QA, b) TAUS Dynamic Quality Framework (DQF).
CAT-QA-08.12	The ***LSRMS Solution*** should allow Users with the appropriate role, access rights and permission to flag and identify segments and documents in the corpus (TM) that are for example; a) Misaligned, b) Lacking in quality* c) Misaligned and lacking in quality, and d) Sensitive in nature based on the security classification level that should be removed from The ***LSRMS Solution***. ***** Lacking in quality - segment found in the TM is a poor translation, badly phrased, incorrect terminology, spelling errors, missing fragments of meaning.

SOW NUM	Requirement (RATED)
CAT-QA-08.13	The ***LSRMS Solution*** should allow Users with the appropriate role, access rights and permission to produce a report of all flagged segments and documents based on the above categories.
CAT-QA-08.14	The report should identify for example; the request number, file name for each flagged segment and/or document, any related metadata and provide a direct link to the segments and/or documents.
CAT-QA-08.15	The flagged segments and/or documents should be added to a queue from which a User with the appropriate role, access rights and permission can validate, realign, replace, delete and modify the content.
CAT-QA-08.16	The ***LSRMS Solution*** should have out of the box document quality evaluation report functionality.
CAT-QA-08.17	The ***LSRMS Solution*** should allow a User with the appropriate role, access rights and permission to create, edit, delete and archive internal Translation Bureau and external resource(s) document quality evaluation reports.
CAT-QA-08.18	The ***LSRMS Solution*** should allow a User with the appropriate role, access rights and permission to configure the parameters for document quality evaluation report for example, the frequency, alerts, notifications, distribution, internal Translation Bureau resource(s) and external resource(s).
CAT-QA-08.19	The ***LSRMS Solution*** be able to perform QA checks not only after the completion of the translation but also on-the-fly or on a segment-by-segment basis.
Web Crawling The following web crawling functionality should be provided;	
CAT- WCRWL-09.1	The ***LSRMS Solution*** should provide web crawling capability to extract and retrieve any text in both official languages from GC websites that have already been translated and published on GC official sites in order to feed the Corpus.
CAT- WCRWL-09.2	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to configure the web crawling parameters.
CAT- WCRWL-09.3	The ***LSRMS Solution*** should notify a User with the proper role, access rights and permission of any web crawling errors or failures.
CAT- WCRWL-09.4	The ***LSRMS Solution*** should log any web crawling errors or failures with a description and time.
CAT- WCRWL-09.5	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to generate reports on any web crawling.
CAT- WCRWL-09.6	The ***LSRMS Solution*** should have the capability to accept any URL and extract any text from different web pages in two languages.

3.8 SECTION G – ANALYTICS, REPORT AND AUDIT (ARA)

3.8.1 Objectives

Analytics, Reporting and Auditing (ARA) section of requirements describes the capabilities of the ***LSRMS Solution*** to ensure there is a technology-driven process for analyzing data and presenting reportable information for Translation, Terminology and Interpretation to a number of different recipients such as executives, managers, other Users and resource(s) .

The ARA requirements encompass a variety of tools, applications and methodologies that should allow PSPC to collect data from the ***LSRMS Solution***, define and run queries against the data, perform audits, prepare the data for analysis, create reports, and dashboards for data visualizations in presenting the analytical results such as on past and current trends, on statistical analysis and information made available to decision makers and operational Users (refer to *Appendix C – Translation Bureau Reports* for a list of Bureau report types)

3.8.2 Requirements

SOW NUM	Requirement (MANDATORY)
ARA-MAN-01	The ***LSRMS Solution*** must have data analysis and analytics capability.
ARA-MAN-01.1	The ***LSRMS Solution*** must provide report capability.
ARA-MAN-01.2	The ***LSRMS Solution*** must provide audit capability.

SOW NUM	Requirement (RATED)
Analytics The ***LSRMS Solution*** should provide analytics functionalities;	
ARA-ANLT-02.1	The analytics information, metadata and data should be available in Canada's Official Languages.
ARA-ANLT-02.2	A User with the proper role, access rights and permission should be able to search, filter, group, view and perform analytics using configurable parameters on: a) All User entered and defined data, and b) All solution captured and stored data.
ARA-ANLT-02.3	To be able to import analytical information, metadata and data in various file formats; a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) JSON, e) CSV file, and f) XML file.
ARA-ANLT-02.4	To be able to export analytical information, metadata and data in various file formats; a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) JSON, e) CSV file, and f) XML file.
ARA-ANLT-02.5	To allow grouping of Translation, Terminology and Interpretation metadata data elements across multiple criteria for example; by TB client, resource(s) , service, contract, location, and time.
ARA-ANLT-02.6	Ability to configure the analytics access rights and permission ,for a User with the proper role, access rights and permission, to restrict for example access, view, search, filter, execution, and distribution of the information, metadata, and data.
ARA-ANLT-02.7	Ability to perform basic searches and filtering, for a User with the proper role, access rights and permission.
ARA-ANLT-02.8	Ability to perform advanced searches and filtering, for a User with the proper role, access rights and permission.

SOW NUM	**Requirement (RATED)**
ARA-ANLT-02.9	Ability to save, print and download analytics information and data, for a User with the proper role, access rights and permission.
ARA-ANLT-02.10	The ***LSRMS Solution*** should provide APIs (Application Programming Interface) for 3rd party analytics tools.
Reports The ***LSRMS Solution*** should provide the following reporting functionalities:	
ARA-RPTG-03.1	The report information, metadata and data should be available in Canada's Official Languages.
ARA-RPTG-03.2	i. Ability to search, filter, group, view, and generate report, for a User with the proper role, access rights and permission using configurable parameters and data for example :All User entered and defined data, and ii. All solution captured and stored data.
ARA-RPTG-03.3	Allow a User with the proper role, access rights and permission to define and generate reports for example; production, productivity, financial, and executive.
ARA-RPTG-03.4	Generate configurable end-to-end workflow reports for Translation, Terminology and Interpretation that reflects the Task and activities for any specified time which can be for example in real time, daily, weekly, monthly.
ARA-RPTG-03.5	Generate configurable reports for Translation, Terminology and Interpretation that reflects the workload for any specified time which can be for example in real time, daily, weekly, monthly, and yearly.
ARA-RPTG-03.6	Generate performance reports based on configurable parameters for example; hardware, operating system, and web applications.
ARA-RPTG-03.7	Allow a User with the proper role, access rights and permission to restrict access, view, report generation, and distribution.
ARA-RPTG-03.8	Generate pre-defined (canned) reports both manually and automatically based on the information and data captured in the solution.
ARA-RPTG-03.9	Generate configurable ad-hoc reports both manually and automatically based on the information and data captured in the solution.
ARA-RPTG-03.10	Generate exception based reports based on filters, data elements, and parameters.
ARA-RPTG-03.11	Generate reports manually or automatically for any specified time for example in real time, daily, weekly, monthly, and yearly, by a User with the proper role, access rights and permission.
ARA-RPTG-03.12	To export pre-defined (canned) report information and data in various file formats by a User with the proper role, access rights and permission; a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) JSON, e) CSV file, and f) XML file.
ARA-RPTG-03.13	To export configurable ad-hoc report information and data in various file formats by a User with the proper role, access rights and permission; a) MS Excel (xls, xlsx), b) MS Word (doc, docx),

SOW NUM	Requirement (RATED)
	c) PDF, d) JSON, e) CSV file, and f) XML file.
ARA-RPTG-03.14	To be able to create and configure the format of the information and data in; a) Tabular, b) Columnar, c) Cross tab or pivoted, and d) Banded. By a User with the proper role, access rights and permission
ARA-RPTG-03.15	To send report manually or automatically at predefined times by a User with the proper role, access rights and permission.
ARA-RPTG-03.16	To send report individually and using a distribution list at predefined times by a User with the proper role, access rights and permission.
ARA-RPTG-03.17	To save, print and download report information and data by a User with the proper role, access rights and permission.
ARA-RPTG-03.18	Provide APIs (Application Programming Interface) for 3rd party report tools.
Audits The following audit capability should be provided;	
ARA-ADT-04.1	The ***LSRMS Solution*** should have auditing functionality to capture in real time any changes within the ***LSRMS Solution***.
ARA-ADT-04.2	The ***LSRMS Solution*** should have auditing functionality to retain the audit history of any changes within the ***LSRMS Solution*** for a specified configurable time period.
ARA-ADT-04.3	The ***LSRMS Solution*** should capture any changes within the ***LSRMS Solution*** with a User name or ID, time stamp and description of the change.
ARA-ADT-04.4	Allow a User with the proper role, access rights and permission to be able to search, filter, group, view, and generate audit using configurable parameters and data on: a) All User entered and defined data, and b) All solution captured and stored data.
ARA-ADT-04.5	Provide the LSRMS Solution audit information, metadata and data in Canada's Official Languages.
ARA-ADT-04.6	The ***LSRMS Solution*** should allow importing of the audit information and data in different formats; a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) Txt, and e) Csv.
ARA-ADT-04.7	The ***LSRMS Solution*** should allow exporting of the audit information and data in different formats; a) MS Excel (xls, xlsx), b) MS Word (doc, docx), c) PDF, d) Txt, and e) Csv.

SOW NUM	**Requirement (RATED)**
ARA-ADT-04.8	Allow a User with the proper role, access rights and permission to restrict access, view, audit generation, and distribution.
ARA-ADT-04.9	Allow a User with the proper role, access rights and permission to save, print and download audit information and data.
ARA-ADT-04.10	The ***LSRMS Solution*** should provide APIs (Application Programming Interface) for 3rd party audit tools.
Dashboard The ***LSRMS Solution*** should provide the following functionalities:	
ARA-DASH-05.1	The dashboard information and data should be available in Canada's Official Languages.
ARA-DASH-05.2	To be able to search, filter, group, view, and generate dashboard using configurable parameters and data on; a) All User entered and defined data, and b) All solution captured and stored data. By a User with the proper role, access rights and permission.
ARA-DASH-05.3	To drag-and-drop data to visualize analytics by a User with the proper role, access rights and permission.
ARA-DASH-05.4	To select from a wide range of charts and tables to display the information and data by a User with the proper role, access rights and permission.
ARA-DASH-05.5	To configure dashboard access rights and permission to restrict access, view, dashboard generation, and distribution by a User with the proper role, access rights and permission.
ARA-DASH-05.6	To tailor the content of embedded dashboards.
ARA-DASH-05.7	To auto-suggest charts and tables based on information and data.
ARA-DASH-05.8	To tailor the layout and display of the information and data.
ARA-DASH-05.9	To save, print and download dashboard information and data by a User with the proper role, access rights and permission.
ARA-DASH-05.10	Provide APIs (Application Programming Interface) for 3rd party dashboard tools.
Business Intelligence Management The ***LSRMS Solution*** should provide the following functionality:	
ARA-BI-06.1	To deliver, enable and support for example; integrated Data warehouse/On-line Analytical Processing (OLAP) capability for business intelligence (BI) and reporting, supporting analytical operations, such as consolidation (roll-up), drill-down, and slicing and dicing.

3.9 SECTION H - DATA AND INFORMATION MANAGEMENT

3.9.1 Objective

The objective of this section is to describe the requirements for data and information management to be provided by the Contractor within the overall scope of the ***LSRMS Solution*** to ensure that;

a) Information needs are met from different perspectives: PSPC Translation Bureau policies, processes and regulations; TB clients from GC Departments and Agencies; stakeholders and partners.

b) Information reaches high quality standards and retains its business value over its lifetime.

c) Information is seamlessly flowing between various systems and databases.

d) Master data is constantly evolving through manual and automated processes.

e) Data assets are preserved from system failures and recovery mechanisms are agreed upon, planned and implemented.

f) Opportunities are present to expand the database architecture in order to respond to changes in regulations and business needs and allow for manual data integrity modifications if required.

3.9.2 Requirements

SOW NUM	Requirement (RATED)
Database Operations Management The ***LSRMS Solution*** should provide the following functionalities:	
DTA-DBOP-01.1	To support the creation and exchange of all open dataset file formats such as CSV, XML, JSON.
DTA-DBOP-01.2	To import data directly from an external source using standard file formats such as CSV, XML, XLS, XLSX, TXT, JSON.
DTA-DBOP-01.3	To export data to external systems using standard file formats such as CSV, XML, XLS, XLSX, TXT, JSON.
DTA-DBOP-01.4	To configure and manage regular (scheduled) and ad hoc import/export processes using a configurable set of search criteria, fields, data formats, grouping and sorting options.
DTA-DBOP-01.5	To configure, schedule and track the following data operations; a) Extracts (exporting), b) Creation of data sets (open data), c) Feeding of target data stores (OLTP, OLAP, SOA), d) Web/online publishing (e.g. HTML/RSS-XML feeds), and e) System/User reports and queries.
Document, Record & Content Management The ***LSRMS Solution*** should provide the following functionalities:	
DTA-INFM-02.1	For the creation and management of document templates which includes; checklists, forms, worksheets that may contain text, format features and fillable form elements, such as text input fields, checkboxes, drop down lists, data tables, tables.
DTA-INFM-02.2	For the creation of new documents through various mechanisms, such as: i. Using a blank or pre-defined template; ii. Importing (upload) an existing document, and iii. Cloning an existing document as a new one.
DTA-INFM-02.3	For metadata information to be captured during the creation of document
DTA-INFM-02.4	For the management of documents to be able to add, edit, and delete.
Metadata Management and Taxonomy The ***LSRMS Solution*** should provide the following functionalities:	
DTA-META-03.1	For the import and export of taxonomy structure and terms using standard formats such as CSV, XML, TXT.
DTA-META-03.2	Allow a User with the proper role, access rights, and permission to define rules on how metadata is captured for each instances of a record, such as: manual keying, dropdown menu feeding from taxonomies or database content, auto-complete.

SOW NUM	Requirement (RATED)
Data Archiving The ***LSRMS Solution*** should allow file data to be archived:	
DTA-ARCH-04.1	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to add, edit, delete file data from the archive.
DTA-ARCH-04.2	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to define the file data archiving rules.
DTA-ARCH-04.3	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to define, customise and configure the metadata for the file data to be archived.
DTA-ARCH-04.4	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to select the type of file data to be archived.
DTA-ARCH-04.5	The ***LSRMS Solution*** should allow file data to be archived automatically based on configurable time.
DTA-ARCH-04.6	The ***LSRMS Solution*** should allow file data to be archived manually.
DTA-ARCH-04.7	The ***LSRMS Solution*** should allow the archived file data to be accessible and retrievable by a User with the proper role, access rights, and permission.
DTA-ARCH-04.8	The ***LSRMS Solution*** should allow a User with the proper role, access rights, and permission to configure the file data retention period.
DTA-ARCH-04.9	The ***LSRMS Solution*** should track file data add, modify and delete with a User name or ID, timestamp and brief description.
DTA-ARCH-04.10	The ***LSRMS Solution*** should allow searches and queries on file data in the archive based on standard and custom filters.
DTA-ARCH-04.11	The ***LSRMS Solution*** should allow standard or custom reports to be generated from the archive.
DTA-ARCH-04.12	The ***LSRMS Solution*** should allow importing and exporting of the reports in various formats.
DTA-ARCH-04.13	The ***LSRMS Solution*** should display error messages, alerts or notification to a User if issues are encountered during the archiving process.
DTA-ARCH-04.14	The ***LSRMS Solution*** error messages, alerts or notification should be logged and retained with the error messages, alerts or notification and time stamp.
DTA-ARCH-04.15	The ***LSRMS Solution*** should allow the archived file data to be encrypted.
DTA-ARCH-04.16	The ***LSRMS Solution*** should allow the archived file data to be compressed.
DTA-ARCH-04.17	The ***LSRMS Solution*** should allow scripts to be used for clean-up of the archive file data based on standard and custom rules, and filters manually and automatically.

3.10 SECTION I - USER MANAGEMENT

3.10.1 Objective

The objective of this section is to describe the requirements for the Contractor to allow PSPC to manage Users.

3.10.2 User Management Requirements and Deliverables

This section includes roles and groups, registration, profiles and accounts, login and credential requirements.

3.10.3 Requirements

SOW NUM	Requirement (MANDATORY)
USR-ROLE-1.0	**Roles / Group** The ***LSRMS Solution*** must provide the capability to manage user roles and groups.
USR-REG-2.0	***Registration*** The ***LSRMS Solution*** must have user registration capability.
USR-ACCT-3.0	***Profiles/Accounts*** The ***LSRMS Solution*** must allow the management of user profiles and accounts.
USR-LOGN-4.0	***Login*** The ***LSRMS Solution*** must authenticate a user at login.
USR-CRED-5.0	***Credentials*** The ***LSRMS Solution*** must provide the capability for a user to use login credentials.

SOW NUM	Requirement (RATED)
Roles / Group The ***LSRMS Solution*** should provide the following functionalities;	
USR-ROLE-01.1	To provide role-based access control that defines the access rights and permission, to features and functionalities in the solution.
USR-ROLE-01.2	For a User with the proper role, access rights and permission to set and administer User types, roles, and groups.
USR-ROLE-01.3	For a User with the proper role, access rights and permission to assign Users to groups.
USR-ROLE-01.4	To allow for a variety of User types, roles, and groups to be defined.
USR-ROLE-01.5	To allow a single User to have multiple roles.
USR-ROLE-01.6	To restrict User to only access information, metadata, and data relevant to User types, roles, and groups.
USR-ROLE-01.7	For a User with the proper role, access rights and permission to add, edit and delete User groups.
USR-ROLE-01.8	For a User with the proper role, access rights and permission to add, edit and delete User to one or more User groups.
USR-ROLE-01.9	For a User with the proper role, access rights and permission to add, edit and delete the access rights to features and functionalities of an individual User at the group level.
USR-ROLE-01.10	For a User with the proper role, access rights and permission to be able to review, validate, add, edit and delete characteristics of a User profile.
USR-ROLE-01.11	For a User with the proper role, access rights and permission to be able to review, validate, add, edit and delete individual settings and characteristics of individual User in groups.
USR-ROLE-01.12	For a User with the proper role, access rights and permission be able to delegate their own role to another User for a configurable period of time.
Registration The ***LSRMS Solution*** should provide the following functionalities:	
USR-REG-02.1	For a User with the proper role, access rights and permission to be able to register a User.

SOW NUM	Requirement (RATED)
USR-REG-02.2	For a User with the proper role, access rights and permission to be able to register.
USR-REG-02.3	To validate user registration information.
Profiles / Accounts The Contractor must deliver a solution that provides the following functionalities:	
USR-ACCT-03.1	To create and manage configurable User profile information which can be used as attributes within the solution for example; region, language preference, time zone, contact details, manager name, and security clearance.
USR-ACCT-03.2	For a User with the proper role, access rights and permission to be able to add, edit, delete, disable, and close individual User profiles in LSRMS.
USR-ACCT-03.3	To retain User account records and information within LSRMS for access by a User with the proper role, access rights and permission for a configurable time period.
USR-ACCT-03.4	For a User with the proper role, access rights and permission to be able to clone User profiles for use by new Users.
USR-ACCT-03.5	For a User with the proper role, access rights and permission to be able to clone User profiles and be able to modify the settings and specific elements of the profiles.
USR-ACCT-03.6	For a User with the proper role, access rights and permission to manage User accounts once they are created for example send notifications to User related to account use, and to update account information.
USR-ACCT-03.7	For a User with the proper role, access rights and permission to be able to add, edit, and delete a User accounts on behalf of a User.
USR-ACCT-03.8	For a User with the proper role, access rights and permission to search, display, add, edit and delete changes to the profile of any User.
USR-ACCT-03.9	For a user with the proper role, access rights and permission to search, display, add, edit and delete changes to an account of any User.
Login The ***LSRMS Solution*** should provide the following functionalities:	
USR-LOGN-04.1	To require a User to authenticate themselves when accessing the ***LSRMS Solution*** and any other applicable components using a User ID and password.
USR-LOGN-04.2	For a User with the proper role, access rights and permission to be able to setup multifactor authentication.
USR-LOGN-04.3	The ***LSRMS Solution*** should allow a User to change and reset the password.
USR-LOGN-04.4	The ***LSRMS Solution*** should prompt a User for old and new password when changing or resetting the password.
USR-LOGN-04.5	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to configure the password character length and rules.
USR-LOGN-04.6	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to configure the number of password reuse.
USR-LOGN-04.7	The ***LSRMS Solution*** should be able to track a User login attempts.
USR-LOGN-04.8	The ***LSRMS Solution*** should be able to lock out a User after a number of failed login attempts.

SOW NUM	Requirement (RATED)
USR-LOGN-04.9	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to set the number of failed login attempts.
USR-LOGN-04.10	The ***LSRMS Solution*** should be able to encrypt the User name and password when the User has submitted the credentials for authentication.
USR-LOGN-04.11	To mask the password as it is entered by the User.
Credentials The ***LSRMS Solution*** should provide the following functionalities:	
USR-CRED-05.1	To directly transfer or upload credentials for authorized Users to the ***LSRMS Solution*** and any other applicable components.
USR-CRED-05.2	Provide the capability to define credentials for authorized Users to the ***LSRMS Solution*** and any other applicable components.

4 TECHNICAL REQUIREMENTS

4.1 INFORMATION TECHNOLOGY AND SOLUTION MAINTENANCE AND UPDATES

4.1.1 LSRMS Hosted Solution

The Contractor must deliver, configure, test, implement, support, and manage in Canada’s Official Languages an ***LSRMS Solution*** including relevant information technology hardware and software components and related business processes to deliver the functional requirements detailed in the SOW.

The LSRMS must accommodate the modification, adjustment, or addition of business process work flows, system automated functions, and other related linguistic management rules and processes without application code changes.

The LSRMS components must have the functionality to integrate with IT components used by PSPC and delivery partners.

The LSRMS must include management and operations support of the scalable, robust, resilient on-demand computing and network infrastructure.

4.2 HARDWARE REQUIREMENTS

PSPC is procuring an ***LSRMS Solution*** as a Contractor Managed Service which uses provider’s applications hosted on Contractor or SubContractor infrastructure.

The Contractor must develop, configure, test, implement, support, maintain and house all infrastructure to support the solution deployed to meet all the requirements defined in the SOW.

4.3 INTEROPERABILITY WITH OTHER SYSTEMS AND ENVIRONMENTS

4.3.1 Background

In order to develop and support streamlined linguistic services, the ***LSRMS Solution*** may require the exchange of information and data with other systems and environments.

This section describes the data exchange requirements for LSRMS and related technical requirements based on current information to:

a) Ensure that the LSRMS aligns with PSPC standards and facilitates interoperability with, PSPC and non PSPC processes, data, systems and environments; and
b) Identify and specify the high level data exchange requirements with other departmental systems and non-PSPC data sources.

The requirements in *Section 4.4 LSRMS Technology Requirements* specifies applicable technology standards, policies, directives and requirements in support of these data exchange requirements in this section.

4.3.2 General System Interoperability

There is a requirement for structured and modular external interfaces which will allow information and data exchange between the ***LSRMS Solution***, other systems and environments through a secure infrastructure.

The interfaces may include:

a) Intranet or extranet
b) Web services such as 3rd party data feeds,
c) COTS 3rd party security components,
d) Other systems containing information and data that is captured for use within the ***LSRMS Solution***,
e) COTS available generic adapters or connectors for interfacing with other systems and environments such as SIGMA.

The Contractor must provide a list of all interfaces affected and 3rd party application interoperability modules and/or Application Programming Interfaces (API) used in the solution.

The Contractor must ensure these APIs are interoperable with PSPC’s systems.

In support of the PSPC’s strategic plans for application interoperability, the ***LSRMS Solution*** must expose its functionality through an API that leverages industry-standard API protocols.

The Contractor must provide an application integration toolkit that other solution providers can leverage for support in creating integration methodologies, as requested by the PSPC, for their applications that includes:

a) Enterprise Application Integration tool in a media and format specified by PSPC.
b) reference documentation (in Canadian English and Canadian French) on tool usage that includes:
c) Original Equipment Manufacturer (OEM) manuals and guides;
d) Instructional documents providing details on controls, methods, data dictionaries, etc.;
e) Best practices and whitepapers;
f) Sample application integration source code;
g) A list of all libraries supported by the ***LSRMS***;
h) An application compliance testing guide that includes:

i. Test cases that PSPC partners can use to assess an application's compliance with supported protocols and standards; and
ii. A compliance checklist that PSPC partners can complete to record and report on compliance testing results.

4.3.3 Technical Interoperability

In support of PSPC's strategic plans for application interoperability, the ***LSRMS Solution*** must expose its functionality through an API that leverages industry-standard API protocols and technologies.

The ***LSRMS Solution*** must interoperate with PSPC's IT stack for example infrastructure and platform as determined and requested by PSPC without significant change to the existing PSPC infrastructure or changes to desktops.

4.3.4 Requirements

SOW NUM	**Requirement (RATED)**
The ***LSRMS Solution*** should provide the following interface functionality:	
TEC-INTFC-01	To create and send information to resource(s) from LSRMS via notifications (email or alerts on the Portal).
TEC-INTFC-02	To support data exchanges to and from legacy systems during the transitional period using PSPC preferred interface frequency, styles and methods: a) Real-Time or batch, b) Web services / APIs, and c) XML and/or Flat file.
TEC-INTG-02	To provide the interface to Sigma using file exchange-based mechanism, specified by SIGMA rather than live API calls due to Sigma network zoning restrictions.
TEC-INTG-02.1	To allow for future integration with various other systems and environments to be determined by the **Client** in collaboration with the Contractor.
TEC-INTG-03	To handle character set encoding for text-based files imported to / exported from the ***LSRMS***.
TEC-INTG-03.1	To encode in UTF-8 any Text, XML or XML-based file generated by the LSRMS unless otherwise specified by Canada.
TEC-INTG-03.2	To encode in UTF-8 or other format as specified in file header any XML or XML-based upload file accepted by the LSRMS unless otherwise specified by Canada.
TEC-INTG-03.3	To provide ability to identify character encoding of the file (e.g. UTF-8, UTF-16, ISO-8859-1, etc.) unless otherwise specified by Canada by any aspect of the LSRMS which accepts uploaded TEXT files.

4.4 LSRMS TECHNOLOGY REQUIREMENTS

4.4.1 Introduction

The LSRMS must be a flexible, scalable and adaptable solution that meets changing business needs mostly through managing configurations available within the solution.

The requirements in this section describe what the solution must deliver, enable and support in terms of technical capabilities that must be met for the solution to co-exist and interoperate.

The versions and the GC or PSPC applications, systems, and tools will be provided when the information is available. As with all other GC policies and standards, the technology standards change and LSRMS is expected to support the technology standard changes as requested by PSPC.

4.4.2 Compliance

The ***LSRMS Solution*** compliance requirements are stated in *Part 2 Legislative, Regulatory and Policy Requirements*.
Requirements in this section are technology specific compliance requirements that the LSRMS must facilitate PSPC's compliance with stated policies, directives and guidelines.

4.4.3 Interoperability

The ***LSRMS Solution*** must allow interoperability as required with for example PSPC, Contractor and 3rd party applications, systems, and tools using the following as a minimum:

a) APIs (out of the box, partially or fully developed),
b) Import and export of ***LSRMS Solution*** data and content.

4.4.4 Usability

Usability is the ease of use and learn-ability of the LSRMS. The usability requirements in this section focus on PSPC and IT industry best practices and standards that have been adopted widely for building and maintaining the easy-to-use Web applications.

4.4.5 Reliability

Requirements in this section specify solution capabilities and architecture that in general give a higher level of availability, more maintainable application and higher overall resiliency.

4.4.6 Scalability

Scalability should be part of the ***LSRMS Solution*** in being able to handle on demand increase in volume without impacting performance.

4.4.7 Requirements

SOW NUM	Requirement (RATED)
The ***LSRMS Solution*** should provide the following functionality;	
TECH-01.1	To interoperate with GC, PSPC, Contractor and 3rd party applications, systems, and tools using the following; a) APIs (out of the box, partially or fully developed), b) Import and export of all ***LSRMS Solution*** data and content.
TECH-01.2	To support the concept of open architecture and allowing accessibility to its services, features and functionalities through other Contractor -provided and/or third-party APIs, Web services, and similar technology.
TECH-01.3	To allow web pages and web feeds encoded in UTF-8 and UTF-16 (Unicode Transformation Format).
TECH-01.4	To support real time interoperability leveraging web services architecture such as; REST (HTTPS bound, JSON and/or XML encoding) and SOAP (HTTPS and/or JMS bound).
TECH-01.5	To allow vertical scaling of physical resource(s) to handle load and on demand increase in volume without rebooting and impacting performance.

SOW NUM	Requirement (RATED)
TECH-01.6	To include load balancing to control and distribute inbound traffic.
TECH-01.7	To support web and application server scalability and performance, tuning functionality should include ; a) Scalability built-in: i. An integrated function, and ii. An external capability. b) Required performance tuning functionality includes, for example: i. Dynamic load balancing; ii Clustering, and iii. Caching of components of the application environment to increase Performance.
TECH-01.8	To provide distinct staging environment(s) as necessary for the purpose of configuring, testing and training for the new software releases.
TECH-01.9	To support the capability of versioning of configurations, and the ability to roll back to previous production versions.
TECH-01.10	To support best practices for securing web services, such as NIST SP 800-95 Guide on Secure Web Services
TECH-01.11	To automatically terminate a web session after a period of inactivity, to be determined by PSPC.
TECH-01.12	To allow any database to manage and protect data up to Protected B level.
TECH-01.13	To support the solution in a segregated network and a zoned environment such that the LSRMS infrastructure is divided into zones respective of trust level such that: a) Logical separation of data is preserved, and b) Physical separation is connected through boundary devices.
TECH-01.14	To allow the current GC Internet Browser standard – Microsoft Internet Explorer 11, and two previous major versions when the standard changes.
TECH-01.15	To allow compatibility with other internet browsers for example Microsoft Edge, Firefox, Safari and Chrome.
TECH-01.16	To support the capability to run as a secure web browser-based solution that does not require any other desktop software and plugins (add-on) to be installed on the User's workstation besides a web browser.
TECH-01.17	To support the capability where a User can navigate directly to an actionable screen from the notification requesting an action, without logging-in again.
TECH-01.18	To support validation and confirmation of data entry by field type, data sizes, table properties and pre-configured list of values for example; only valid postal code format will be accepted for postal code.
TECH-01.19	To support the architecture style that enables robust error handling, recovery and notification to a User when online errors occur.
TECH-01.20	To support best practice W3C Web Application Best design principles for usability for example; enabling/disabling buttons, options and flows based on User entered values, and reducing needless prompting.
TECH-01.21	To support One-Time Login (Single Sign On – SSO), for GC User, to provide role-based access to all components of the LSRMS.

SOW NUM	Requirement (RATED)
TECH-01.22	To support the current GC operating system (OS) Microsoft Windows 7 Enterprise version and up.
TECH-01.23	To support the capability of securing data in transit with Hypertext Transfer Protocol Secure (HTTPS), and Transport Layer Security (TLS 1.2 or above), supporting the encryption requirements in 5.3.9 (Security Requirements – Encryption)
TECH-01.24	The ***LSRMS Solution*** servers should be storage persistent to prevent changes written to disc from being lost in the event the server is turned off or on through planned or unplanned activity.
TECH-01.25	The ***LSRMS Solution*** should allow a User with the proper role, access rights and permission to monitor physical server resource(s) utilization in real time.
TECH-01.26	The ***LSRMS Solution*** hardware-assisted virtualization hypervisor should be segregated from other virtualization hypervisors.
TECH-01.27	The ***LSRMS Solution*** should allow the portability of the virtual machine (VM).
TECH-01.28	The ***LSRMS Solution*** VM should be backed up.
TECH-01.29	The ***LSRMS Solution*** should allow the capability to restore a VM to a previous state in time.
TECH-01.30	The ***LSRMS Solution*** should allow the capability to identify virtual machines via policy tags/metadata.
TECH-01.31	The ***LSRMS Solution*** uptime and response time should be monitored in real time.
TECH-01.32	The ***LSRMS Solution*** network bandwidth utilization should be monitored in real time.
TECH-01.33	The ***LSRMS Solution*** should monitor the database and include; a) I/O utilization, b) Query performance (execution - success and error), c) Throughput, and d) Latency.
TECH-01.34	The ***LSRMS Solution*** should accommodate 2000 concurrent Users.
TECH-01.35	The ***LSRMS Solution*** should include performance metrics to monitor the following; a) Application, b) Operating system (OS), c) Virtualization, d) Network, and e) Database
TECH-01.36	The ***LSRMS Solution*** should allow a User with the proper access rights and permission to view performance reports on the following; a) Application, b) Operating system (OS), c) Virtualization, d) Network, and e) Database.
TECH-01.37	The ***LSRMS Solution*** should allow a User with the proper access rights and permission to customize the view of performance reports on the following; a) Application, b) Operating system (OS), c) Virtualization, d) Network, and e) Database.

SOW NUM	Requirement (RATED)
TECH-01.38	The ***LSRMS Solution*** should allow a User with the proper access rights and permission to generate performance reports on the following; a) Application, b) Operating system (OS), c) Virtualization, d) Network, and e) Database.
TECH-01.39	The ***LSRMS Solution*** should capture events, threshold violations, errors, warnings, alerts and include the ID, type, time stamp, and description to the following; a) Application, b) Operating system (OS), c) Virtualization, d) Network, and e) Database
TECH-01.40	The ***LSRMS Solution*** should allow a User with the proper access rights and permission to customize performance reports to; a) Application, b) Operating system (OS), c) Virtualization, d) Network, and e) Database.
TECH-01.41	The Contractor should identify, to PSPC, any scale or access limitations that may take effect during any stage of the contract or while meeting scalability and performance requirements.
TECH-01-42	The network connection between the PSPC and the ***LSRMS Solution*** should provide a connection of 1GBit/Sec or more.

5 NON-FUNCTIONAL REQUIREMENTS

5.1 CONTEXT

This part is to identify outcomes or requirements that are applicable across all aspects of the ***LSRMS Solution***.

5.2 HIGH LEVEL COMMITMENTS

5.2.1 Ability to Adapt to Change

The ***LSRMS Solution*** must be able to adapt and accommodate to change from the PSPC on an agreed to timeline. PSPC anticipates that the following possible types of changes are likely to occur within the life of the Contract**:**

a) Adding a new or modifying an existing workflow to accommodate new policies or approaches in the Translation Bureau processes.
b) Adding a new or modifying an existing data element to accommodate new reporting requirements or changes to existing data dictionaries.
c) Adding new or modifying the existing content of communications messages.

d) Importing and/or exporting information with new or existing systems or services.
e) Modifying policies and administrative requirements.
f) Adding or modifying existing connectors and APIs.

While PSPC anticipates that there may be change management costs for resource(s) and activities related to modifying the flexible and configurable ***LSRMS***, the information technology capacity required of the Contractor as described in *Part 5 Non-Functional Requirements* clearly lays out requirements for a flexible solution that is able to evolve over time without incurring significant information technology change management costs.

5.2.2 Solution Flexibility

The Contractor must have the ability to access the ***LSRMS Solution***, when authorized by the Technical Authority, to develop workarounds to modify or suspend standard operations. In such cases, the Contractor must:

a) Document process changes.
b) Maintain complete records impacted by the change, and
c) Develop adhoc reports to quantify and qualify changes as a result of the modified or suspended processes.

Accommodating Policy Driven Changes
Changes to the environment, policies and processes are frequent. The LSRMS must be flexible enough to adapt to changes and be able to modify the workflows, data fields, processes, and configurations accordingly as specified by Government of Canada.

5.2.3 Solution Usability

The Contractor must adopt and leverage best practices in solution design, for example:

a) Ensure consistent and standardized User interface in the ***LSRMS Solution***,
b) Guide the User by providing context sensitive help messages and visual process maps available when requested by PSPC,
c) Intuitive User interface design by adhering to best practices in web, such as make interactive objects obvious, give feedback, never have User repeat anything, always have default values in fields and forms,
d) Incorporating best practice web application usability tools and plug-ins, such as mouse-over details, auto-complete/suggest, calendar scheduler, multi-select combo box, date picker, drag and drop manager, hot-keys,
e) Smooth integration with productivity tools and desktop environment, such as drag and drop capability with MS Office products suite,
f) Allow a User to create hyperlinks to any document so that it can be referenced anywhere within the solution, and
g) Allow a User to personalize and manage their own views. This includes for example; creating favorites, short-cuts, setting default actions, and default values for business processes and data.

5.2.4 Principles of Effective Information Management

Information Management is an integral part of the Contractor's responsibilities. Key Performance Indicators (KPI) and transactional data allows the Translation Bureau to measure and report on performance, create new policies and maintain high quality client service at all stages of the project (request) lifecycle.

The Contractor must apply the basic principles of effective information management to:

a) Avoid unnecessary collection of duplicate information, reconcile inconsistencies and ensure data quality,
b) Ensure that information is complete, accurate, current, relevant, and understandable,

c) Support access to information subject to policy and legal requirements,
d) Prevent unlawful access to information, and
e) Safeguard information against loss, theft and damage.

The Contractor, must provide details to PSPC on:

f) What and how information is to be captured and used,
g) How long a program or service will operate, and
h) How long the information will be needed for operational and legal / evidence purposes.

5.3 SECURITY REQUIREMENTS

5.3.1 Security

Appendix G – Security and Privacy will detail security requirements and the Security Requirements Traceability Matrix (SRTM).

The Contractor must ensure that the LSRMS datacenters, LSRMS software, LSRMS middleware, LSRMS service desk, Security Operations Centre (SOC) and Network Operations Centre (NOC) infrastructure and data for the entire LSRMS must reside in Canada.

The Contractor must ensure that all work under the Contract (including SOC, NOC and service desk) performed by Contractor personnel, whether through SubContractor or otherwise, be performed within Canada.

The Contractor must ensure any business entity conducting work under the Contract have a physical location within Canada.

5.3.2 Personal Information

The *Privacy Act* places limits on the collection, use and disclosure of personal information by federal government institutions. It also gives Canadians the right to access and correct personal information about them that is held by institutions.

The Contractor must safeguard all personal and protected information, for example the following:

a) Translation Bureau resource(s) identification information,
b) Translation Bureau resource(s) Financial information,
c) Procedures, forms, computer systems and data file layouts, and Internet Web sites, etc.,
d) Contact information (including business/company name), biographical information, educational information, financial information, security clearance information, evaluations/assessments, other identification number (e.g. Business Number) and signature, and
e) Translation (TB client) documents containing personal information.

5.3.3 Protected Information

The Contractor must:

a) Be responsible for the safekeeping, protection and privacy of this information, and upon close-out of the Contract, returning all information to the PSPC,
b) Ensure that the conversion, imaging and subsequent destruction of any personal information originating from the Contract is conducted in accordance with all applicable legislation and policies, and
c) Safeguard any information created, destroyed, stored, accessed and modified in the delivery of the solution in accordance with legislated requirements. In doing so, the ***LSRMS solution*** must:

i. Ensure that the quality, accuracy, completeness and integrity of the data within the ***LSRMS Solution*** is always maintained through the use of appropriate validation measures,
ii. Ensure that the consistency of the data is both reconcilable and auditable,
iii. maintain a multi-channel history of information sent or received, information exchanged, and account updates performed by or on behalf of the TB client,
iv. Protect sensitive information and safeguard against theft, including identity theft or unauthorized third parties acting on behalf of TB clients, fraud or disclosure as per the *Privacy Act*, and
v. Ensure any destruction of records is completed following the standards set out in the *Library and Archives Act* and LSRMS Disposition Authority.

5.3.4 SA&A Program and SA&A Compliance

The Contractor must participate in the Security Assessment and Authorization (SA&A) program as it relates to the ***LSRMS Solution***. The SA&A program is based upon the Information System Security Implementation Process (ISSIP) for more details refer to *Part 6: PSPC Security Assessment and Authorization (SA&A) Process*.

5.3.5 Risk Management

The Contractor must maintain the security posture of the solution through continuous monitoring and annual audit of the implemented security requirements. This includes, for example:

a) Monitoring Threats and Vulnerabilities,
b) Proactive Threat mitigation measures,
c) Reporting any security issues to the PSPC IT Security Coordinator immediately upon learning of their existence, and
d) Tracking and reporting progress to the PSPC IT Security Coordinator until each security issue is fixed or mitigated.

5.3.6 Access Control

The Contractor must have a process to manage and monitor privileged access to the solution for example:

a) Enforcing and auditing approved authorizations for logical access to the solution,
b) Granting and limiting access only to authorized devices and Users with an explicit need to have access,
c) Monitoring for unauthorized remote access or remote management and expeditiously disconnecting or disabling unauthorized remote access,
d) Routing of all remote access through a limited number of managed access control points.
e) Implementing multifactor authentication for privileged data center accounts that includes proper separation of duties, role based access, and least-privilege access, and
f) Authorization of execution of privileged commands and access to security-relevant information only for operational needs.

The Access Control (AC) family of the SCP contains further details regarding the Access Control requirements (refer to *Appendix G – Security and Privacy).*

5.3.7 *LSRMS Solution*, Information, Data and Services

The Contractor will be required to demonstrate within 60 days after Contract Award its compliance with PSPC's request that the ***LSRMS Solution***, data, information, and services will reside entirely in Canada.

The Contractor must restrict the location of information processing, information/data, and information system services to Canada (refer to *Appendix G – Security and Privacy).*

5.3.8 Disclosure

The information system must not release information outside of the established system boundary or to any 3rd party unless PSPC security safeguards and procedures are used to validate the appropriateness of the information designated for release (refer to *Appendix G – Security and Privacy).*

5.3.9 Encryption

The solution must protect all data at rest and in transit with encryption (refer to *Appendix G – Security and Privacy.* The Contractor must ensure that any cryptography used to implement safeguards or as part of authentication mechanism for example TLS, software modules, Public Key Infrastructure (PKI), and authentication tokens where applicable) is configured for use with CSE approved cryptographic algorithms and cryptographic key sizes and crypto periods.

This includes, for example:

a) Cryptographic algorithms, cryptographic key sizes and crypto periods that have been approved by CSE and validated by the Cryptographic Algorithm Validation Program (CAVP) and are specified in ITSP.40.111 or in a subsequent version,
b) Implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (CMVP) to at least FIPS (Federal Information Processing Standard) 140-2 validation at Level 1, and
c) Operate in FIPS Approved Mode of Operation.

5.3.10 Data Leakage

The Contractor 's solution must implement controls to ensure appropriate isolation of resource(s) such that PSPC data is not co-mingled with other tenant data without compensating controls, while in use, storage or transit, and throughout all aspects of the solution's functionality and system administration.

This includes implementing access controls and enforcing appropriate logical and physical segregation to support:

a) The separation between the Contractor 's internal administration from resource(s) used by PSPC, and
b) The separation of customer resource(s) in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another.

5.3.11 Least Functionality

The Contractor must configure the information system to provide only essential capabilities (refer to *Appendix G – Security and Privacy.*

Where feasible the Contractor must limit component functionality to a single function per device and should disable unused or unnecessary physical and logical ports/protocols (such as USB, FTP, IPv6, HTTP).

5.3.12 Incident Response

The Contractor must work with the PSPC IT Security Coordinator and the PSPC Departmental Security Officer (DSO) on Security Incident containment, eradication and recovery in accordance with the Contractor and PSPC Incident Response processes.

This includes, for example, the ability for PSPC to track the status of reported information security events, to request and receive discrete access and information associated with PSPC Data (User data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.) in an unencrypted fashion for the purposes of conducting investigations and the ability for PSPC to track the status of a reported information security event.

The Contractor must alert and notify the PSPC IT Security Coordinator (via phone and email) of detected suspicious events or unusual activities with security implications.

The Incident Response (IR) family of the SCP contains further details regarding the Contractor's IR role and responsibilities (refer to *Appendix G – Security and Privacy).*

5.3.13 Audit

The Contractor must work with PSPC for the development and implementation of audit functions, analysis and reporting. The Contractor's solution and service must facilitate audit functions including, the following:

a) The Contractor PSPC Access to audit information without Contractor assistance,
b) Protection of audit information and audit tools from unauthorized access, modification ordeletion,
c) Sufficient audit storage capacity to ensure audit storage capacity is not exceeded which could result in the loss or reduction of auditing capability,
d) The solution alerts Contractor personnel of audit failures including taking automatic actions predetermined by PSPC and alerting key stakeholders when audit capacity reaches 75%,
e) The Contractor notifies PSPC of any audit failures, and
f) The solution must have the ability to forward events and logs to an PSPC (or any 3rd party contracted by PSPC) managed centralized audit log system using standardized reporting interfaces, protocols and data formats for example common event format (CEF), syslog, or other common log formats, APIs that support log data remote retrieval.

The Audit and Accountability (AU) family of the SCP contains further details regarding audit requirements (refer to *Appendix G – Security and Privacy*).

5.3.14 Security Control Profile (SCP)

The SCP defines the security controls required of the Contractor ***LSRMS Solution***.

The Contractor must provide a comprehensive approach to security for the ***LSRMS Solution*** and service throughout the Term of the Contract.

To ensure that adequate security controls are in place, PSPC has developed a baseline SCP based upon the controls and methodologies from the Communications Security Establishment (CSE) guidance document: ITSG-33, IT Security Risk Management: A Lifecycle Approach (requirements (refer to *Appendix G – Security and Privacy SCP controls)*

5.3.15 Evidence

As part of PSPC's SA&A process the Contractor must provide an explanation of how their organization and/or ***LSRMS Solution*** meet the security control profile. Detailed evidence of compliance to each control will be required during the SA&A program and the suitability of the evidence will be assessed by PSPC's IT Security Coordinator.

The following are required as a component of the Contractor's Security Requirement Traceability Matrix (SRTM), and SubContractor Report on the SA&A compliance of the solution refer to *Appendix G – Security and Privacy* section *14.2* for more information:

a) If a control or line item is Not Applicable (NA) to the Contractor 's ***LSRMS Solution*** the Contractor must NOT remove the line item and must provide a justification for the NA status,
b) If the control or line item is applicable to the Contractor 's ***LSRMS Solution*** but is NA to a partner/sub-Contractor , the Contractor must provide a justification for the NA status in relation to the partner/sub-Contractor ,
c) The Contractor must indicate if a partner/sub-Contractor is responsible for the implementation of the control, and
d) The Contractor must provide an explanation of how their organization and ***LSRMS Solution*** meet the security control.

5.3.16 IT Security Certifications

The Contractor must maintain any certification and audit standards, provided as part of its bid, during the entire Term of the Contract.

The Contractor must, for the Term of the Contract, provide hosting services supplied by either the Contractor or SubContractor service provider holding a valid certification such as ISO 27001/27002:2013, ISO/IEC 27018, FedRAMP, and such certification must be issued by a reputable certification body such as a certification body employing CASCO standards.
If compliance to an SCP control is established through a certification provided by a Subcontratctor, the Contractor must supply a copy of the Certificate and/or the Certification Report for example: Designated Organizational Screening: PROT B from Public Services and Procurement Canada (PSPC)

If compliance to an SCP control is established through security clearances for relevant personnel, the Contractor must provide:

a) List of all clearances for relevant personnel,
b) Name of the originating organization for the security clearance, and
c) File number (#), date of issuance, and date of expiry.

5.3.17 Requirements

SOW NUM	Requirement (MANDATORY)
SEC-MAN- 01	**Data Residency and Personnel** The Contractor must clearly demonstrate its data residency compliance and provide a data center deployment plan(s) which should include specifics on: a) Location(s) (country and city) of primary data center(s); b) Location(s) (country and city) of secondary data center(s) and backup centers;

SOW NUM	Requirement (MANDATORY)
	c) Location(s) (country and city) of all the infrastructure components (including, for example, database servers, SANS, application servers); and d) Location(s) (country and city) of the SOC, NOC and the Service Desk. The Contractor must clearly demonstrate its business entities and personnel location compliance and provide: e) Location(s) (country and city) of all business entities performing Work under the Contract; and f) Location(s) of all personnel performing the Work under the Contract.
SEC-MAN-02	**Secure Web Connection** The Contractor must implement safeguards to ensure that all publicly accessible government websites and web services are configured to provide service only through a secure connection, in accordance with Section 6.2.4 of the Policy on the Management of Information Technology and the Policy on Government Security. a) Contractor will implement a secure web connection that: • Is configured for HTTPS • Has HSTS enabled • Implements TLS 1.2, or subsequent versions, and uses supported cryptographic algorithms and certificates, as outlined in CSE's • ITSP.40.062 Guidance on Securely Configuring Network Protocols, Section 3.1 for AES cipher suites • ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information • disables known-weak protocols such as all versions of Secure Sockets Layer (SSL) (e.g. SSLv2 and SSLv3) and older versions of TLS (e.g. TLS 1.0 and TLS 1.1), as per CSE ITSP.40.062 • disables known-weak ciphers (e.g. RC4 and 3DES)

SOW NUM	Requirement (RATED)
SEC-03	**IT Security Policies and Procedures (Controls)** The Contractor should demonstrate its ability to comply with the IT security requirements by maintaining policies and procedures that support IT security throughout the Contract by providing evidence of any existing policies and procedures that support the security control families described in Appendix G and ITSG-33. The Contractor should describe how its policies and procedures align to the security control families by providing the following information on current policies and procedures: (a) Name of policy and/or procedure, (b) Its purpose,

SOW NUM	Requirement (RATED)
	(c) Its scope, (d) The roles and responsibilities that are described within the policy and/or procedure, (e) How it ensures coordination among organizational entities, and (f) How it ensures compliance within the organization. Note: The Contractor should provide sufficient detail with regard to its policies and procedures in order for Canada to evaluate this response in full.
SEC-04	**IT Security Topology Diagram** The Contractor should provide an IT security topology diagram which should include the following components: a) Interfaces - separate bullet for each category, b) Web, c) Applications, d) Databases, e) Security devices, f) System management, and g) Backup infrastructure.
SEC-05	**Security Organization** The Contractor should describe the experience of the security organization that will be responsible in ensuring the security of the LSRMS Solution, including the name of each person, their role and description of their duties, their experience, and certifications.
SEC-06	**Data Segregation** The Contractor should provide its proposed approach to data segregation, that should include: a) Information system design documentation; b) Information system architecture; and c) Process and procedures to support data segregation.
SEC-07	**Disposal and Sanitization** The Contractor should provide its proposed approach to the disposal and sanitization of Canada's data, including: a) A plan for hard-drive sanitation or an action plan if the system is hosted in a virtual environment that will ensure Canada's data is not obtainable; b) A plan for data disposal; c) System disposal processes and procedures; d) A plan for destruction of duplicate records that may be stored in a records management system or backups; and e) The process it plans to follow when the system is no longer required and is being decommissioned.
SEC-08	**Continuous Monitoring Service** The Contractor should provide its proposed approach to continuous monitoring and include the following components: a) The strategy for continuous monitoring,

SOW NUM	Requirement (RATED)
	b) Established measures, metrics, and status monitoring and control assessments frequencies, c) Details of data collection and its reporting aspects, d) Analysis methods of the data gathered and Report findings accompanied by recommendations, e) Response mechanisms to assessment findings to include making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority, and f) Review and update cycles to support continuous improvement and maturing measurement capabilities.

SEC-09	**Industry IT Security Certification**
	The Contractor should provide proof of its security certification(s) and applicable audit standards for its proposed solution in the form of a copy of a valid certificate or audit standard and describe how the certification or audit standard was assessed and obtained for each IT Security certification and audit standard held, such as:
	a) FedRAMP;
	b) Cloud Security Alliance – STAR;
	c) COBIT;
	d) ISO 27001;
	e) PCI DSS;
	f) CMM; and
	g) Others.
	The Contractor should also stipulate if the certification or audit standard applies to the whole solution or to a specified portion of their solution.

SEC-10	**Identity, Credential and Access Management** The Contractor should provide details on its proposed solution’s Identity, Credential and Access Management level of assurance capabilities with respect to TBS Standard on Identity and Credential Assurance. The Contractor should identify the level of assurance and demonstrate how it meets the requirements of that level.

5.4 SERVICE MANAGEMENT

5.4.1 Context

Service Management is the strategic approach to designing, delivering, managing and improving the way information technology (IT) will be used within the ***LSRMS Solution***. The goal of Service Management is to ensure that the right processes, people and technology are in place so that the ***LSRMS Solution*** can meet the business goals of PSPC. Service Management is associated with Information Technology Infrastructure Library (ITIL), a framework that provides best practices for aligning IT with business needs.

The Contractor must manage its IT services and deploy a set of specialized resource(s) and capabilities equivalent to those prescribed by the ITIL framework as a source of best practice in service management. The framework must emphasize the importance of coordination and control across the various functions, processes, and systems necessary to manage the full life cycle of IT Services including the strategy, development, design, transition, operation and continual improvement—The IT Service Management Lifecycle (ITSM).

The Contractor must provide audit reports to the Project Authority as requested by PSPC, conducted by an independent organization to demonstrate alignment with best practices, actions taken to address gaps, and continued compliance.

The Contractor must adapt the ITIL Guidance (or similar framework) to support the LSRMS environment, and must continually deploy these practices for the duration of the Contract.

5.4.2 ITSM Incident, Problem, Change, Release Management

The following table identifies the ITSM best practices high level process and activities the Contractor should provide in collaboration with PSPC for incident, problem, change, and release management:

Process	Activities (Steps)
1.0 Incident Management	a) Incident identification b) Incident logging c) Incident categorization d) Incident prioritization e) Analysis, and diagnosis f) Escalation to another tier support level g) Tracking h) Communication with PSPC technical support throughout the life of the incident i) Incident resolution j) Incident closure, and report(s).
2.0 Problem Management	a) Problem detection b) Problem logging c) Problem categorization d) Problem prioritization e) Problem investigation, analysis, and diagnosis f) Creating a known error record g) Communication with PSPC technical support throughout the life of the problem h) Problem resolution i) Closure and reports(s) and Major problem review

Process	Activities (Steps)
3.0 Change Management	a) Creating a Request for Change (RFC)/ Change Request (CR) b) Reviewing and assessing a Request for Change c) Change management support d) Change assessment by the change manager e) Change assessment by the Change Advisory Board (CAB) f) Change scheduling and build authorization g) Assessment and implementation of change(s) h) Testing the Change i) Change deployment authorization j) Change deployment k) Post implementation review and change closure
4.0 Release Management	a) Release management support b) Release and deployment planning c) Release building and testing d) Release package Deployment e) Early life support f) Release review and closure a deployment

5.4.3 Service Levels Requirements

5.4.3.1 Performance Measurement and Reporting

The Contractor must provide a Performance Report to the Project Authority on a monthly basis containing statistical information on the performance of the ***LSRMS Solution*** as compared to the requirements set out in the SOW.

The report must include the service request identifier, the service request status and information that the Project Authority requires to understand the service request and its resolution.

5.4.3.2 Service Standard Failures and Exclusions

With respect to Service Standard Failures or a negative trend towards failing to meet the Service Standards, upon conducting an analysis of the data captured in the Performance Report, the Contractor must identify any discrepancies, including:

a) Notify the Project Authority as soon as the Contractor becomes aware of such failure,
b) Carry out a root cause analysis to investigate the underlying cause of the failure and preserve any data indicating the cause of the failure,
c) Take action as agreed with the Project Authority to minimize the impact of the failure and prevent it from recurring,
d) If practical, correct the failure immediately in order to resume fulfillment of the Service to the applicable Service Standard,
e) Prepare and deliver to the Project Authority a report identifying the failure and, where possible, its cause, business impact, remedial plans, timeframe for implementing improvement plans, and any impact on the Services,
f) Advise the Project Authority of the status of all remedial efforts being undertaken by the Contractor with respect to the underlying cause of the failure, and
g) In calculating the Contractor ’s compliance with the Service Standards, any performance issues:

Caused by factors outside of the Contractor ’s control, that resulted from any actions or inactions of GC or any third parties not within the Contractor ’s control, or

i. That resulted from PSPC’s equipment and/or 3rd party equipment not within the primary control of the Contractor these must not be included in such calculations (unless the event is the result of acts or omissions of the Contractor).

At the PSPC’s request, the Contractor must provide substantiation that the cause of the service issue is reasonably outside of its control.

5.4.4 Service Standards

5.4.4.1 Application Availability

This service level measures the availability of the ***LSRMS Solution***.

APPLICATION AVAILABILITY		
Service Measure	**Performance Target**	**SLR Performance %**
a) Percentage	The percentage of time that the application is available for normal business operations. (24:00 to 24:00 EST, 7 days a week)	Production Applications: 97.0%
b) Formula	Number of minutes during the month being reported on when the production applications and their various components were operating without any Priority Level One or Two incidents within the control of the Contractor divided by the Total number of minutes during such month minus (number of minutes of maintenance window + planned downtime)] multiplied by 100 = [percentage of availability of the application during such month.	
c) Measurement Interval	Calendar month	
d) Reporting Period	Calendar month	
e) Measurement Method/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including either uptime or downtime data.	

5.4.4.2 Contractor Reporting

This service level identifies the adherence of the Contractor to the agreed schedule and accuracy of reports, as identified in the SOW.

REPORTING		
Service Measure	**Performance Target**	**SLR Performance %**
a) Reporting Schedule	Provision of reports, as identified in the SOW, within the defined time lines in of the Contract	95%
b) Formula	Schedule Adherence (%) is based on the number of agreed actions that are completed within the target dates, divided by the total number of agreed actions in the measurement period.	

REPORTING	
	Accuracy (%) is based on the number of individual reported data elements that are in line with actuals, divided by the total number of data elements contained in all reports presented within the month.
c) Measurement Interval	Calendar month
d) Reporting Period	Calendar month
e) Measurement Method/Source Data	To be determined by PSPC in consultation with the Contractor after Contract Award and accepted by the TB Client.

5.4.4.3 Contractor LSRMS Service Desk Availability

SERVICE DESK AVAILABILITY		
Service Measure	**Performance Target**	**SLR Performance %**
a) Schedule	TBD by GC in consultation with the Contractor after Contract Award	95%
b) Formula	Availability (%) = 100% - Unavailability (%) where Unavailability is defined as: (Σ Outage Duration × 100%) ÷ (Schedule Time - Planned Outage)	
c) Measurement Interval	First month: Measure daily Thereafter: Measure daily	
d) Reporting Period	First month: Report weekly Thereafter: Report monthly	
e) Measurement Method/Source Data	To be determined by PSPC in consultation with the Contractor after Contract Award and accepted by the **Client**.	

5.4.4.4 Contractor LSRMS Service Desk Incident Acceptance Response Time

Incident Acceptance Response Time is the measure of the time for the service desk to accept (i.e., receive, log and assign for Resolution) an Incident. Time is measured from the time the Incident is received by the Contractor to the time it is logged and assigned for resolution in the service desk application.

INCIDENT ACCEPTANCE RESPONSE TIME		
Service Measure	**Performance Target**	**SLR Performance %**
a) Percentage	Priority 1 Incident: ≤ 60 elapsed minutes Priority 2 Incident: ≤ 60 elapsed minutes Priority 3 Incident: ≤ 2 Standard Operating Hours Priority 4 Incident: ≤ 4 Standard Operating Hours	≥ 90% (all Priority Levels)
b) Formula	Number of Incidents (of all Priority Levels) received and accepted (i.e., received, logged, and assigned) within the Target Performance during the Measurement Interval divided by Total number of Incidents (of all Priority Levels) received and accepted during the Measurement Interval] multiplied by 100% = “Percent (%) Attained”	

INCIDENT ACCEPTANCE RESPONSE TIME	
c) Measurement Interval	Calendar month
d) Reporting Period	Calendar month
e) Measurement Method/Source Data	To be determined by PSPC in consultation with the Contractor after Contract Award and accepted by the **Client**.

5.4.4.5 Contractor Requirements

SOW NUM	**Requirement (MANDATORY)**
SRV-STD-01	Planned maintenance must occur between 24:00. Friday and 6:00 Monday, Eastern Standard Time.
SRV-STD-02	In the event of unplanned maintenance, the Contractor must obtain acceptance from the contract technical authority on when such unplanned maintenance may occur.
SRV-STD-03	If the Contractor must conduct any emergency maintenance, the Contractor must immediately notify, in writing, the Technical Authority, who must approve the maintenance before it is conducted.

5.4.5 Service Desk

5.4.5.1 Context

The service desk is the single point of entry and contact for TB clients and Users. It is a key function in assisting and resolving issues, in restoring normal service operation as quickly as possible minimizing the adverse impact on business operations, and ensuring that the best possible levels of service quality and availability are maintained.

Incident Management handles all incidents which come in many forms and can be related to application, hardware and network issues all of which must be rectified in a timely manner to minimize impacts to the business.

Incidents are usually addressed in the moment (reactive) when they are reported however, depending on the nature, complexity and impact of the issue there may be a need to involve or escalate to other support levels (tiers) for resolution.

Through the incident management process a more proactive approach can be taken to resolve recurring incidents that have an unknown root cause by using the problem management process.

The key activities of the problem management process are to diagnose the root cause of incidents identified through the incident management process, and to determine the resolution or work around to those problems.

Once this has been accomplished, the resolution or work around is implemented through the appropriate control procedures of change and release management.

5.4.5.2 Objectives

The objectives of the incident, problem, release and change management processes are to:

a) Restore normal service operation as quickly as possible and minimize the adverse impact on

Business operations,

b) Prevent problems and resulting incidents from happening,
c) Eliminate recurring incidents,
d) Minimize the impact of incidents that cannot be prevented,
e) Minimize the negative impact when changes are implemented,
f) Provide TB clients with a consistent high-quality experience, Adopt standard process and use tools based on industry best practices, and
g) Define and measure the critical KPIs that will drive improvement in the processes.

5.4.5.3 Service Manager

The Contractor must provide a Service Manager that must be available to meet with PSPC representatives during business days from 08:00 to 17:00 EST to deal with release implementation activities, release maintenance and release window scheduling, service quality, management services escalation (Incidents),and service reporting, and be reachable outside of theses hours for high priority Incidents, urgencies, and security Incidents.

5.4.5.4 Service Desk Structure

The Contractor must provide and maintain an English and French service desk, be accessible and available (see table below) by PSPC technical support to address, resolve and escalate ***LSRMS Solution*** and any 3rd party issues.

Support Level	Weekdays	Regular Hours (EST)	After Hours (EST)	Weekend	After Hours (EST)
PSPC Support L1	Mon to Fri	8:00 to 17:00	17:00 to 8:00	Fri to Mon	17:00 to 8:00
PSPC Support L2					
Contractor Support L3*					
*Contractor – support for ***LSRMS Solution*** and any SubContractors, Partners or 3rd party tools.					

5.4.5.5 Service Desk Requirements

SOW NUM	Requirement (MANDATORY)
SRV-DESK-01	The Contractor must have a Service Desk accessible via a toll-free number, e-mail and website using a contact method, to respond to incidents and service requests (the “Support Request”). The Technical Authority will provide the Contractor with a list of Users authorized to issue support requests.
SRV-DESK-02	The Contractor must provide and maintain a bilingual (English and French) service desk accessible by PSPC to provide support and help in the use of ***LSRMS Solution***, to respond to inquiries, networking, hardware, software, database and security management support requests, to resolve service disruptions, and User issues related to non-working features or functionalities.
SRV-DESK-03	The service desk must collaborate with PSPC technical support staff in the resolution of LSRMS problems, that would include Contractor or PSPC 3rd party tools and PSPC systems integrated as part of the ***LSRMS Solution***.

SOW NUM	Requirement (MANDATORY)
SRV-DESK-04	The Contractor must collaborate with PSPC in determining the support structure, processes and procedures that will be used for escalation, incident, problem and change management based on an agreed upon model.
SRV-DESK-05	The Contractor must have support processes defined and practiced for escalation, incident, problem, and change management.
SRV-DESK-06	The Contractor must provide a trouble ticket system to track support requests.

SOW NUM	Requirement (RATED)
SRV-DESK-07	The trouble ticket system should have the ability to provide the following minimum functionalities: a) Generate a unique tracking number, b) An automatic notification via e-mail to the authorized User who issued the support request when a ticket is updated, modified or escalated, c) Ability to generate a monthly report of all trouble tickets created during the month, which includes the information set out in 5.5.4.3, d) Ability to generate additional reports upon the request of PSPC, within a specified time for example, five (5) calendar days after such request, and e) Issue broadcasts or other notices to provide status updates, for planned and unplanned events.
SRV-DESK-08	The trouble ticket should contain the following minimum information: a) Date and time of support request, b) Name of individual submitting the support request, c) Name of individual logging the request, d) Severity level of the support request in accordance with the Contractor ’s, e) Procedures as agreed with the technical authority, f) Provide a description of the problem, g) Detail the affected services, h) The duration of outage, if any, i) The time it took to resolve the problem, j) Comments, and k) Indicate the time and date the problem was resolved.
SRV-DESK-09	The trouble ticket system should have the ability to generate reports: a) Generate a service desk performance report to demonstrate the degree of adherence to service level requirements (SLRs) and to service level agreement (SLA), b) Ability to generate a monthly report of all trouble tickets created during the month, which includes the information set out in 5.5.4.3, c) Ability to generate additional reports upon the request of PSPC, within a specified time for example, five (5) calendar days after such request, d) Track/manage/report service desk utilization, and e) A set of standard reports for example, incident management reporting, problem management reporting and service reports that have already been configured for quick-and-easy use.
SRV-DESK-10	The Contractor service desk employees must meet security clearances and be proficient in ***Canada's Official Languages***.

SOW NUM	Requirement (RATED)
SRV-DESK-11	The Contractor should provide all necessary skilled resource(s) and staff with the proper security clearance, and language proficiency during planned and unplanned events.
SRV-DESK-12	The Contractor should provide all necessary skilled resource(s) and staff with the proper security clearance, and language proficiency to support and operate the bilingual service desk.
SRV-DESK-13	The Contractor should provide trained technical service desk staff for tier 1, tier 2, and tier 3 support for escalation including those escalated to 3rd parties, inquiries, incident and problem resolution.
SRV-DESK-14	The Contractor should have documented service desk operations and administration procedures.
SRV-DESK-15	The Contractor should maintain and provide updated escalation contact list(s) for all service tiers (including 3rd parties) throughout the contract period to PSPC upon request.
SRV-DESK-16	The Contractor should provide a closure-loop process for incident management and be able to communicate and inform PSPC technical support staff or Users on status changes or be able to contact PSPC technical support staff or Users for more information if required.
SRV-DESK-17	The Contractor should provide an after-hours number for issues reported by PSPC support see section 5.4.5.4 – Service Desk Structure

5.4.5.6 First Point of Contact

The Contractor must act as a first point of contact for all incidents, problems and general communication from PSPC technical support and provide the following support including:

a) Perform identification, logging, categorization, prioritization, initial diagnosis, escalation to other support tiers, resolution, closure, and communication with PSPC technical support staff throughout the life of the incident,
b) Restoring ‘normal service operation’ as quickly as possible in the case of disruption,
c) Assisting PSPC technical support staff by managing communication and escalating incidents and requests using defined procedures,
d) Resolving incidents related to software, hardware, and network issues,
e) Responding to application incidents and provide “how to” support,
f) Provide password support for Contractor provided credentials (if applicable), including self-service password reset capabilities, requests for account privilege change requests, requests for User account activation, suspension and termination,
g) Resolving problems related to unknown cause of one or more incidents,
h) Provide First Point of Contact (FPOC) contact access via toll-free telephone number, email, self-serve, live chat, and ticketing system for all service desk Services described in this SOW, and
i) Provide multiple alternative support request delivery channels see section below for Support Request Delivery Channels (SRDC).
j) Support Request Delivery Channels (SRDC)

The Contractor must provide a service desk that is accessible and available in all Canadian time zones through a number of different support request delivery channels such as:

SOW NUM	Requirement (RATED)
SRDC-TEL-01	**Telephone** The Contractor should provide a local and toll-free phone line allowing PSPC technical support staff, to speak directly with service desk support staff to submit and resolve support request such as inquiries, how to, and service incident.
SRDC-AA-02	**Automated Attendant (AA)** The Contractor should provide an Automated Attendant (AA) service channel that present PSPC technical support staff, with an array of self-service options.
SRDC-AA-02.1	The AA service should be provided in ***Canada's Official Languages*** 24 hours a day, 7 days a week.
SRDC-AA-02.2	PSPC technical support staff, should have the option of speaking to service desk support at any point during operating hours.
SRDC-AA-02.3	The AA should include: a) Prompt response: to answer all calls on the first ring, b) User service: 24 hours a day, 7 days a week, c) Call redirection: use a simple menu to route callers to the appropriate telephone number or recorded information without any personal assistance. Recorded information can be updated at any time from any telephone, and is password protected, d) Message service: hold the call for a specific extension if it rings busy, announce the caller's position in queue and offer the options to stay in queue, leave a message, leave a call back number or hang up and try again later, and e) Ability to perform administrative functions, "how to" support through User access to knowledge bases and online Incident status checking.
SRDC-EML-03	**Email** Providing an e-mail address or web form allowing PSPC technical support staff to use their email program to submit incidents.
SRDC-EML-03.1	The Contractor should provide confirmation and notifications via e-mail to PSPC technical support staff or User who contact the service desk via e-mail.
SRDC-LIVE-04	**Live Chat** The Contractor should provide chat session, allowing PSPC technical support staff, to open a text dialogue.
SRDC-DISA-05	**Persons with Disabilities** The Contractor should provide alternative formats for all TB client-oriented communications and services to TB clients as required.
SRDC-DISA-05.1	The Contractor should ensure that service desk technology is updated and incorporated into the overall TB client service
SRDC-FAQ-06	**Frequently Asked Questions** The ***LSRMS Solution*** should allow PSPC technical support staff, to reference a list of common questions and answers that can leverage a knowledge base.

5.4.5.7 Incident Priority Level, Business Impact and Description

The following table defines the incident priority levels, business impact and description:

Priority Level		Business Impact	Description
P1	Critical	Critical Business Impact or National Interest	The Incident has caused a complete and immediate work stoppage affecting a critical function or critical infrastructure component, and a primary business process or a broad group of User. No workaround available. Examples: a) Major application problem (e.g., cataloguing, sourcing, etc.) b) Severe disruption during critical periods (e.g., fiscal year end processing) c) Network outage d) Security breach violation In addition, Priority Level 1 must be assigned to Incidents pertaining to national interest.
P2	High	Major Business Impact	A business process is affected in such a way that business functions are severely degraded, multiple User are impacted, a key Authorized User is affected, or a critical function is operating at a significantly reduced capacity or functionality. A workaround may be available, but is not easily sustainable. Examples: a) Major data/database or application problem, and b) System is performing slowly, but workload is manageable. Security incursion on a non-critical system.
P3	Medium	Moderate Business Impact	A business process is affected in such a way that certain functions are unavailable to User or the LSRMS and/or service is degraded. A workaround may be available.
P4	Low	Minimal Business Impact	An Incident that has little impact on normal business processes and can be handled on a scheduled basis. A workaround is available or there is minimal negative impact on a User's ability to perform their normal daily work. Example: a) "How to" questions, b) Service requests (e.g., system enhancement), *c)* Peripheral problems (e.g., locally attached printer), and d) Preventative maintenance.

5.4.5.8 Incident Response, Resolution Targets and Service Levels

The following table defines the incident priority levels, response, target response and acknowledgement time, target resolution time and service target:

Priority Level		Response	Target Response & Acknowledgement Time	Target Resolution Time	Service Target**
P1	Critical	Immediate and sustained effort, using all available resource(s) until resolved. On-call procedures activated, vendor support invoked.	30 minutes; 24x7	6 hours	90%
P2	High	Support Team responds immediately, assess the situation, may interrupt other staff working normal or moderate priority jobs for assistance.	1 hour; 24x7	1 business day	90%
P3	Medium	Respond using standard procedures and operating within normal supervisory management structures	4 hours; 12x5	2 business days	90%
P4	Low	Respond using standard operating procedures as time allows	6 hours; 12x5	5 business days	90%
**Service Levels are measured against 9 Core Business Hours (8:00 – 17:00), except for P1 – based on a 24-hr clock.					

5.4.5.9 Incident and Problem Management

The Contractor must manage ***LSRMS Solution*** incidents and problems to ensure the rapid restoration of services including:

a) Recommend Incident Management procedures derived from the ITIL or ISO processes
b) Ensure that responses to PSPC technical support staff are based on priority and impact, rather than the method used to notify the service desk (e.g., by telephone, email, fax).
c) Escalate to the Contractor service desk through a defined and agreed upon process,
d) Provide a system to document, manage and track all Incidents, Incident reports and inquiries, regardless of the means by which the incidents are submitted.
e) Provide an end-to-end Incident identification, escalation, transfer, resolution (management) and closure process with PSPC, including Incidents escalated to 3rd Parties.
f) Receive, track, answer and resolve, or monitor to closure, PSPC technical support staff and User calls, email, self-serve, live chat, and ticketing system.
g) Ensure that all Incidents are identified by a unique number regardless of the contact method in order to make them traceable throughout the lifecycle of the service request.
h) Follow the problem management process best practices to:
   i. Ensure that recurring Incidents that meet defined criteria are reviewed using Root Cause Analysis processes.

ii. Document solutions to re-occurring incidents in the knowledge database with the exception of security incidents.

i) Verify acceptance of services by contacting the PSPC technical support staff to confirm results and level of satisfaction.

j) Provide authorization from PSPC technical support staff for closing of service requests and service desk Incidents.

k) Provide to PSPC complete and continuous access to all requests, incident and problem closure information and data such as:

i. Incident/Problem receipt;
ii. Incident/ Problem identification;
iii. Incident/ Problem logging, tracking and updating methods
iv. Incident/ Problem categorization;
v. Incident/ Problem prioritization;
vi. Incident/ Problem management;
vii. Incident/ Problem assignment;
viii. Incident/ Problem resolution and closing.

5.5 WEB ACCESSIBILITY

Persons with Disabilities: The GC is committed to ensuring public accessibility for persons with visual, auditory, mobility and cognitive impairments.

In accordance with GC policies on Accessibility and Usability, the Contractor must provide alternative formats for all client-oriented communications and services to clients as required.

The Contractor must ensure that service desk technology is updated and incorporated into the overall client services.

5.5.1 Web Accessibility

The Standards on Web Accessibility and Web Usability took effect on August 1, 2011, and September 28, 2011, respectfully and were updated on March 31, 2013.

The new standards replaced Part 2 of the Common Look and Feel 2.0 Standards for the Internet. The new standards are known as Web Content Accessibility Guidelines (WCAG) 2.0.

In accordance with the Standard on Web Accessibility, the Contractor should ensure each web page of the LSRMS meets all five WCAG 2.0 conformance requirements.

Conformance requirement level 1 should meet level AA conformance in full. Prior to the commencement of any operational activity for example pilots, and go-live.

Canada will assess the LSRMS's compliance with the WCAG 2.0 conformance requirements. If the LSRMS fails to achieve compliance with the WCAG 2.0 conformance requirements, the Contractor should develop a strategy and timeline for reaching the compliance score for acceptance by the PSPC and must take corrective actions to achieve compliance.

During the compliance assessment, Canada may determine that critical elements of the WCAG 2.0 conformance requirements should be met prior to the commencement of any operation activity. Once corrective actions have been completed for the critical elements, Canada will reassess to ensure compliance has been met.

As per section 2.2 of the Standards on Web Accessibility, the requirements surrounding Accessibility applies to Web pages:

a) That is public-facing (i.e., available to individuals and businesses outside of the GC i.e. freelance translators and interpreters, academia);
b) For which the department is accountable; and
c) That are provided through GC Web applications.

Similarly, as per section 2.2 of the Standards on Web Usability, the requirements surrounding Usability apply to all GC websites and web applications that are:

a) Public-facing (i.e., available to individuals and businesses outside of the GC); and
b) Those for which the department is accountable.

The ***LSRMS Solution*** is a business application. As a public-facing application, it is mandatory that the GC Self-Service Portal adheres to the requirements of the Web Standards for the Government of Canada, the application's User interface, should meet the suggested guidelines of the Standards on Web Accessibility outlined in section *5.5 - Web Accessibility*.

5.5.2 WCAG 2.0 Conformance Requirements

a) Conformance requirement 1 (Conformance Level) defines the levels of conformance.
It can only be met if the following are true:
   i. Level AA conformance is met in full.
   ii. Common failures are avoided for all applicable success criteria.
   iii. Sufficient techniques are used to meet all applicable success criteria.
   iv. Sufficient techniques specific to each technology (that is relied upon) are used where applicable.

b) Conformance requirement 2 (Full pages) defines what needs to be assessed for a Web page.

c) Conformance requirement 3 (Complete processes) defines what needs to be assessed for a Web page that is part of a process.

d) Conformance requirement 4 (Only Accessibility-Supported Ways of Using Technologies) defines the ways of using technologies that can be relied upon to satisfy the success criteria. It can only be met by use of the following technologies:
   i. XHTML 1.0 or later excluding deprecated elements and attributes, HTML 4.01 excluding deprecated elements and attributes,
   ii. HTML5 or later excluding obsolete features, or
   iii. Technologies with sufficient techniques (specific to each technology) to meet all applicable success criteria.

e) Conformance requirement 5 (Non-Interference) defines requirements for ways of using technologies which are not relied upon to satisfy the success criteria.

Section	Standard	Url

2.2	Standard on Web Accessibility (Mar-13)	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601&section=text
2.2	Standard on Web Usability (Mar-13)	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=24227&section=text
6.1.1	Standard on Web Accessibility (Mar-13)	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601&section=text

6 MANAGEMENT AND OVERSIGHT

6.1 CONTEXT

Part 6 describes the PSPC's oversight and contract management requirements and expectations. PSPC's overall aim is to ensure a consistent approach to training, communications, transition and steady-state operations. GC will work jointly with the Contractor to establish an active and ongoing collaborative relationship that is essential to achieving the overall ***LSRMS Solution*** objectives.

6.2 GOVERNANCE EXPECTATIONS – MANAGEMENT APPROACH

The Contractor must work with PSPC to develop a governance and Contract management structure and plan that meets PSPC's expectations and requirements of this Contract.

6.2.1 Management/Governance Principles

The management and governance principles must be defined within the context of the following overarching principles:

a) Stewardship: activities and processes to safeguard money, assets, databases and other knowledge and data assets and protect them against losses, misuses and waste;
b) Transparency: measureable outcomes-based results, performance metrics and reporting;
c) Efficiency/timeliness: a solution that demonstrates successful, efficient change management and results in improved service delivery; and
d) Flexibility: a solution and delivery of services that demonstrates innovation with a focus on flexibility to accommodate multi-layered change and continual service improvement.

6.2.2 Planning Principles

For each plan, the Contractor must:

a) Consult and collaborate with PSPC in the development of the plan and incorporate the considerations, dependencies, constraints, and stakeholders identified by PSPC,
b) Use a logical sequence, which would allow the proper level of communications to all stakeholders, in order to support the PSPC stakeholders through a change management process of iteratively moving to an ***LSRMS Solution***. This involves the active participation of the Contractor in the governance established by the PSPC for change management and issue escalation i.e.: Change Advisory Board,
c) Include a Responsible, Approver, Consulted, and Informed (RACI) chart to identify the roles and responsibilities for key Contractor , PSPC and any 3rd party members involved for the successful execution of the plan,
d) Provide a list of Task dependencies,
e) Identify the phases, gates, deliverables and milestones of the Work as distinct Tasks where each Task has a start and end date, a duration, is assigned to a resource(s) group, and has the dependencies identified, such that the start and end date of the Tasks are driven by the dependencies, duration and resource(s),,
f) Identify each Contract deliverable as a milestone,
g) Schedule Tasks in parallel to the maximum extent possible,
h) Provide a list of planning assumptions, and
i) Identify risks including:
    i. Categorization of each risk;

ii. Probability of each risk;
iii. Impact if the risk materializes;
iv. Mitigation measures and risk response;
v. Monitoring measures; and
vi. Risk assignment.

6.3 PROJECT PLANS

6.3.1 Project Management Plan

The Contractor must provide with the bid response a draft Project Management Plan, which includes the Transition-In Plan that was proposed as part of the Contractor's bid submission and a complete Project Management Plan within 20 business days following Contract Award for review and acceptance by the Project Authority.

The project management plan must address and integrate all the project management knowledge areas as defined in PMBOK edition 5 or PRINCE2 and must include the following:

a) Executive summary description of the ***LSRMS Solution***, components and its services,

b) Organizational plan that includes management structure, organizations, and detailed descriptions of roles and responsibilities and qualifications of key project personnel and subject matter experts The descriptions must address the education; training; experience pertinent to the function; availability and replacement schedule; and responsibility,

c) Resource plan for determining resource(s) levels required to complete the work under the Contract and for assessing the security of the resource(s) to perform the required function. The Contractor must indicate what additional resource(s) they would have available for deployment in case the level of effort being required beyond that which was originally estimated for the above,

d) Contract Work Breakdown Structure (CWBS) at the activity level which must show the relationships between the infrastructure, and all related services in the planning and control of cost, schedule and technical performance. The relationship between the Contract Work Breakdown Structure and organizational responsibilities must be explained,

e) Change management and control plan that defines standard methods and procedure to manage change and supports the planning and controlling of cost, schedule, and technical performance, and to report accurate status against plan, and to forecast results of alternative project actions. The ***LSRMS Solution*** must be extended to cover Work performed by the SubContractor's if applicable,

f) Subcontract Management Plan that identifies the working relationships between the different SubContractors involved in the Work and relationship with the Contractor. Relations with SubContractors must be described in detail. Methods for control and monitoring of SubContractors performance must be described. Methods by which SubContractor are selected, and conditions under which a sub-Contractor may be replaced must be detailed. The Contractor must define the SubContractor interfaces with functional areas of the Contractor organization, and their participation in project progress review updates with the Project Authority,

g) A Project Schedule which will clearly identify activities, events, and their logical or technical links required for the achievement of key project milestones including the Transition-in plan , and will clearly relate to the Contract Work Breakdown Structure and the change control system,

h) Communication Management plan which should include the PSPC – Contractor management of the business relationship, reporting and working with PSPC to resolve service standard exceptions, problems and issues, communication documents, communication needs, joint planning, proposed terms of reference(s) for any joint committees (including frequency of meetings), communicating upcoming changes and their potential impact to User, feedback mechanism, escalation matrix and communication strategy,

i) System Engineering Management Plan, which must ensure that the elements of the CWBS and technical Tasks are correctly identified and controlled, and that the design is complete in its response to all stated needs of GC. It must describe how the requirements are mapped to the planned design and service offering; outlines supporting evidence for claimed performance and scalability; and outline how the responsibility of technical requirements will be distributed among the Contractor , and GC; and a description of the formal design and configuration review process including roles of SubContractors,

j) Quality Assurance (QA) Plan that includes an approach to formulating and enforcing work and quality standards, and reviewing work in progress. The plan must address, for example:

   i. A detailed description of the Contractor 's QA methodology, processes and procedures, and its alignment with a recognized quality management system;
   ii. QA requirements for the implementation and all transition activities, including proposed baseline performance requirements;
   iii. A description of the QA organization;
   iv. The collateral demands on PSPC project staff time for participation in the overall QA program,
   v. The interfaces between the Contractor 's QA functions and those of its SubContractors, and how the responsibilities are allocated;
   vi. Procedural and contractual remedies for recovery of quality problems must be specified for consideration by the Project Authority as components in the final QA program.

k) Risk Management Plan that includes the approach for identifying and tracking risks, isolating the event triggers for risks, assessing probability and impact, as well as identifying a mitigation plan,

l) Issue Management Plan that includes the approach for identifying and managing service management issues, isolating the issues, assessing the impacts, identifying responsible parties, assessment of a severity and priorities, and processes for determining a resolution,

m) Performance management plan including metrics that are based on well-established project management methodologies as defined in PMBOK 5th edition or PRINCE2, to track the scope, schedule, and cost parameters,

n) Release Management Plan related to implementing changes to the service and covers infrastructure and supporting documentation such as specifications, policies, procedures and training material.

6.4 Privacy Management

6.4.1 Privacy Management Plan

The Contractor must provide to the Project Authority a Privacy Management Plan within 45 business days of Contract Award for review and acceptance by the Project Authority.

As a minimum, the Privacy Management Plan must include:

a) Contractor 's privacy protection strategies and detail of exactly how the Personal Information will be treated over its life cycle;
b) How the Personal Information will be collected, used, retained, disclosed and disposed only for the purposes of the Work specified in the Contract;
c) How the Personal Information and Records will be accessible only to authorized individuals (on a need-to-know basis) for the purposes of the Work specified in the Contract;
d) The privacy breach protocol and details on how any privacy breaches will be handled;
e) How the Contractor will ensure that Canadian Privacy requirements, as outlined in the Privacy Act, the Access to Information Act and Library and Archives of Canada Act, will be met throughout the performance of the work and for the duration of the Contract;
f) Any new measures the Contractor will implement in order to safeguard the Personal Information and the records in accordance with their security classification;
g) How the Contractor will ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification; and
h) How the Contractor will ensure that their staff is trained on privacy and privacy related principles.

6.4.2 Privacy Management Plan delivery

The Contractor must implement the Privacy Management Plan (all processes, procedures, roles, and responsibilities), and any subsequent annual updates.

The Contractor must provide to PSPC within 30 business days of a request by the Project Authority, evidence not older than 12 months for example test results, evaluations, and audits to ensure that the Privacy Management Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting the PSPC's privacy requirements.

If changes to the ***LSRMS Solution*** environment are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by the Project Authority, the Contractor must provide PSPC with sufficient detail to support an update to the Privacy Impact Assessment, and obtain acceptance from the Project Authority for the anticipated change.

The Contractor must provide within 60 business days of Contract Award a privacy awareness guide instructing the Contractor's resource(s) regarding the use of the Personal Information provided by PSPC about the User.

6.4.3 Privacy Impact Assessment

The Contractor must provide the requested assistance to PSPC in creating the Privacy Impact Assessment in accordance with the TBS Directive on Privacy Impact Assessment (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308) and provide the following information within 20 business days of a request by PSPC:

a) Business processes, data flows and procedures for the collection, transmission, processing, storage, disposal and access to information including Personal Information;
b) A list of the Personal Information used by the Contractor in connection with the Work and the purpose of each Personal Information item;
c) How the Personal Information is shared and with whom;
d) A list of all secured locations where hard copies of Personal Information are stored;
e) A list of all secured locations where Personal Information in machine-readable format is stored for example, the location where any server housing a database including any Personal Information is located), including back-ups;
f) A list of all measures being taken by the Contractor to secure the Personal Information and the Records beyond those required by the Contract;
g) Any privacy-specific security requirements or recommendations that need to be addressed;
h) A detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and
i) Results of consultations (if any) from a privacy impact assessment review by the Office of the Privacy Commissioner of Canada (OPC) with signoff by OPC.

The Contractor must implement the recommendations from the Privacy Impact Assessment based on a schedule approved by PSPC.

If changes to LSRMS Solution are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by PSPC, the Contractor must provide PSPC with sufficient detail on the changes to support an update to the Privacy Impact Assessment, and obtain acceptance from Project Authority for the anticipated change.

The Contractor must provide a privacy awareness communications kit to Contractor resource(s) involved in the LSRMS Solution that provides an overview on the use, collection and disclosure of Personal Information.

6.5 IT SECURITY MANAGEMENT

6.5.1 IT Security Operations Centre

The Contractor must provide a Security Operations Centre (SOC), prior to the deployment of any functionality to production, with the infrastructure and resource(s) required for the centralized monitoring and resolution (24 hours per day, 7 days per week, and 365 days per year) of the LSRMS security Incidents.

The Security Operations Center (SOC) must:

a) Coordinate security Incidents responses in close coordination with PSPC,
b) Include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year and answered using the official languages of PSPC (English and French) as requested by the caller,
c) Act as a point of contact for communications with PSPC representatives for security Incidents,
d) Not impact operations of the LSRMS in case of a Contractor SOC failure, and

e) Notify GC within 15 minutes if Contractor SOC is not available and provide a contact name that GC can communicate as necessary during the Contractor SOC outage.

The SOC must collaborate with PSPC's Information Protection Centre for activities that include: integration of processes; oversight; security incident handling and response; and auditing.

The SOC must accept emails from User to a Contractor -provided mailbox with an auto reply to confirm receipt of the email. The SOC personnel must acknowledge receipt of emails received within 15 minutes of receiving the email .The SOC must authenticate the identity of the requester using a process accepted by PSPC.

6.5.2 IT Security Plan

The IT Security Plan must describe how the security requirements will be addressed in alignment with PSPC Security Assessment and Authorization (SA&A) process, as described in section *6.6 PSPC Security Assessment and Authorization (SA&A) Process* of this SOW. The Contractor must submit the IT Security Plan within 45 business days of contract award. PSPC Security Assessment and Authorization process is comprised of three gates plus the operational state which provide assessment opportunities at different levels of granularity. It is important to note that all security requirements must be traced from High-level design to Integrate & Test and finally operations. As well, since the controls are dependent upon the solution architecture, the controls at each Gate must be refined by the Contractor, to the satisfaction of PSPC, during the SA&A process.

6.5.3 Service Continuity and Disaster Recovery Plan

The Contractor must update, as requested by PSPC, the draft Service Continuity Plan submitted with its bid based upon feedback from the Project Authority. The Contractor must submit a revised Service Continuity and Disaster Recovery Plan for acceptance.

6.5.4 Technical Architecture Diagrams

The Contractor must update, as requested by PSPC, the draft Technical Architecture Diagrams submitted with its bid based upon feedback from the Project Authority. The Contractor must submit a revised Technical Architecture Diagrams for acceptance.

6.5.5 Technical Integration Approach

The Contractor must update, as requested by PSPC, the draft Technical Architecture Approach submitted with its bid based upon feedback from the Project Authority. The Contractor must submit a revised Technical Integration Approach for acceptance.

6.6 PSPC SECURITY ASSESSMENT AND AUTHORIZATION (SA&A) PROCESS

The SA&A process must be completed in its entirety, and to the satisfaction of PSPC, prior to the commencement of any operational activity such as pilots, and go-live including production transactions and data.

Thereafter, with each release or change management implementation, the SA&A process must be repeated and documented.

To ensure the quality and timely development of the security deliverables, the Contractor must contract the services of a SubContractor SA&A Compliance Specialist per to function as the point of contact for SA&A activities.

The SubContractors SA&A Compliance Specialist will assess the Contractor's compliance to the principles and controls in the Security Control Profile (SCP).

In order to ensure that adequate security controls are in place, PSPC has developed a baseline Security Control Profile (SCP) refer to *Appendix G* based upon the controls and methodologies from the Communications Security Establishment (CSE) guidance document: ITSG-33, IT Security Risk Management: A Lifecycle Approach https://www.cse-cst.gc.ca/en/publication/itsg-33.

PSPC is the final authority on the sufficiency of evidence supplied in support of compliance and the ***LSRMS Solution***, should PSPC discover, through the SA&A process, security risks that are deemed unacceptable by PSPC, at its own discretion, may exercise any rights or remedies to which PSPC is entitled under the Contract (including the right to terminate the Contract for default).

The Contractor must supply a timeline that outlines when he will meet the security Gates in alignment to their Transition – In plan and IT Security plan.

6.6.1 Security Assessment and Authorization Gate 1

The Contractor must complete the following work for SA&A Gate 1:

a) Security Detailed Service Design (SDSD), and
b) Security Requirements Traceability Matrix (SRTM).

All work will be subject to acceptance by the Project Authority.

6.6.1.1 Security High Level Service Design

The Contractor must provide a Security High Level Service Design (SHLSD) that includes:

a) A high-level component diagram that clearly shows the allocation of services and components to network security zones and identifies key security related data flows;
b) The architectural layers for example, communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer;
c) A description of the network zone perimeter defences;
d) A description of the use of virtualization technologies, where applicable;
e) Descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers;
f) Descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements; and
g) A description of the approach for:

i. Access Control
ii. Audit and Accountability
iii. Configuration Management
iv. Contingency Planning
v. Identification and Authentication
vi. Incident Response
vii. Media Protection
viii. Personnel Security
ix. Physical and Environmental Protection
x. Risk Assessment
xi. Security Awareness and Training
xii. System and Communications Protection
xiii. System and Information Integrity
xiv. System Maintenance
xv. System and Services Acquisition

6.6.1.2 Security Requirements Traceability Matrix

The Contractor must provide a SRTM to PSPC that includes for each requirement in *Appendix G – Security and Privacy* section *14.2* for more information:

a) The security control requirement identifier,
b) The security control requirement family or name,
c) The security control requirement number,
d) Description of the security control,
e) Evidence which outlines how the security control requirement is addressed in the Security High-Level Design in sufficient detail to allow the PSPC to confirm that the security safeguards satisfy the security requirements (refer to *Appendix G – Security and Privacy* section *14.2* for more information), and
f) Tracing (a reference to an identifiable element) to the Security Detailed Level Service Design to allow PSPC to confirm that the security safeguards satisfy the security requirements.

6.6.2 Security Assessment and Authorization Gate 2

The Contractor must complete the following work for SA&A Gate 2, following acceptance of the work for SA&A Gate 1, which includes PSPC acceptance for:

a) Security High Level Service Design (SHLSD),
b) Security Requirements Traceability Matrix (SRTM),
c) Change Management Procedures,
d) Operational Security Procedures, and
e) Security Installation Procedures.

6.6.2.1 Security High Level Service Design (SHLSD);

The Contractor must provide a SHLSD that includes:

a) A detailed component diagram (this must be a refinement of the high-level component diagram),
b) Descriptions of the allocation of technical security mechanisms to detailed service design elements,
c) Descriptions of the allocation of non-technical security mechanisms to high-level organizational or operational elements, and
d) Justification for key design decisions

The SHLSD must comply with the Security High Level Service Design.

6.6.2.2 Updated Security Requirements Traceability Matrix

The Contractor must update the SRTM to include the following information for each security requirement in *Appendix G – Security and Privacy* section *14.2* for more information:

a) The security control requirement identifier,
b) The security control requirement family or name,
c) The security control requirement number,
d) Description of the security control,
e) Evidence which outlines how the security control requirement is addressed in the Security High-Level Design in sufficient detail to allow the PSPC to confirm that the security safeguards satisfy the security requirements (refer to *Appendix G – Security and Privacy* section *14.2* for more information), and

f) Tracing (a reference to an identifiable element) to the Security High Level Service Design to allow PSPC to confirm that the security safeguards satisfy the security requirements.

6.6.2.3 Operational Security Procedures

The Contractor must provide Operational Security Procedures to PSPC that includes:

a) For each operator role:
   i. Schedule of security-relevant actions to be performed in order to maintain the security posture of LSRMS Solution,
   ii. How to use available operational interfaces, and
   iii. Each scheduled action and how the User is expected to perform it.

b) Operational roles and responsibilities for:
   i. Interaction requirements with PSPC representatives,
   ii. Reporting schedule and procedures,
   iii. Access control,
   iv. Audit and accountability,
   v. Identification and authentication,
   vi. System and communications protection,
   vii. Awareness and training,
   viii. Configuration management,
   ix. Contingency planning,
   x. Incident response,
   xi. Maintenance,
   xii. Media protection,
   xiii. Physical and environment protection,
   xiv. Personnel security, and
   xv. System and information integrity.

6.6.2.4 Security Installation Procedures

The Contractor must provide Security Installation Procedures details to PSPC that includes:

a) Procedures necessary for the secure installation and configuration of the ***LSRMS Solution*** and all connected components,
b) Installation and configuration of all technical security solutions,
c) Security configuration of hardware products, and
d) Security configuration of software products (COTS and open source).

6.6.3 Security Assessment and Authorization Gate 3

The Contractor must complete the following work for SA&A Gate 3, following acceptance of the work for SA&A Gate 2, which includes PSPC acceptance for:

a) Security Installation Verification Plan,
b) Security Installation Verification Report,
c) Updated SRTM with Security Installation Verification mapping to security requirements,
d) Security Integration Test Plan,
e) Security Integration Test Report,

f) Updated SRTM with Security Integration Test Report mapping to security requirements,
g) Vulnerability Assessment Plan,
h) Vulnerability Assessment Report, and
i) Updated SRTM with Vulnerability Assessment Report mapping to security requirements.

6.6.3.1 Security Installation Verification Plan

The Contractor must provide a Security Installation Verification Plan as part of the IT Security Plan submission to PSPC that must include:

a) The security verification approach;
b) PSPC witnessing arrangements;
c) An outline of the security verification items; and
d) For each security verification item:
    i. A description of the verification scenario;
    ii. Ordering dependencies; and
    iii. Expected results (i.e., pass/fail criteria).

The Contractor must provide an updated SRTM to PSPC that includes for each security requirement to be tested by the Security Installation Verification Plan, the tracing (a reference to an identifiable element) to security installation verification test cases.

The Contractor must conduct security installation verification in accordance with the accepted Security Installation Verification Plan.

The Contractor must correct installation and configuration errors and omissions that are detected as a result of the security installation verification.

6.6.3.2 Security Installation Verification Report

The Security Installation Verification Report must include for each of the test items in the security installation verification plan:

a) The expected results (i.e., pass/fail criteria);
b) The actual results; and
c) A description of deviations and how each was resolved.

6.6.3.3 Security Integration Test Plan

The Contractor must provide a Security Integration Test Plan as part of the IT Security Plan submission to PSPC for acceptance that must include:

a) the security functions to be tested;
b) PSPC witnessing the testing arrangements; and
c) for each security function or sets of security functions, the items to be tested, including:
    i. A description of the test case, procedure, or scenario;
    ii. Environmental requirements;
    iii. Ordering dependencies; and

iv. Expected results (i.e., pass/fail criteria).

The Contractor must provide an updated SRTM to PSPC that includes for each security requirement to be tested by the Security Integration Test Plan, the tracing (a reference to an identifiable element) to integration security testing test cases.

The Contractor must conduct security integration testing in accordance with the Security Integration Test Plan.

6.6.3.4 Security Integration Test Report

The Security Integration Test Report must include, for each of the test items in the Integration Security Test Plan:

a) The expected results (i.e., pass/fail criteria);
b) The actual results; and
c) A description of deviations and how each was resolved.

6.6.3.5 Vulnerability Assessment Plan

The Contractor must provide a Vulnerability Assessment Plan as part of the IT Security Plan submission to PSPC for acceptance and must include:

a) A description of the scope of the vulnerability assessment,
b) PSPC witnessing arrangements,
c) A description of the vulnerability assessment process, and
d) A description of the vulnerability assessment tools that will be used, including any software versions.

The Contractor must conduct a vulnerability assessment in accordance with the accepted Vulnerability Assessment Plan.

The Contractor must implement patches and corrective measures as part of vulnerability assessment activity. Where this is not feasible for example, time to test patch or determine and test corrective measures would seriously delay the project, the Contractor must create Service Request Tickets for any required patch or corrective measure that cannot be implemented as part of the vulnerability assessment activity.

6.6.3.6 Vulnerability Assessment Report

The Vulnerability Assessment Report must include:

a) A listing of the vulnerability assessment tests that were conducted;
b) All raw data for the results of the vulnerability assessment tests in a COTS file formats and names specified by PSPC;
c) For each vulnerability assessment test:
    i. Whether a known vulnerability was detected,
    ii. A description of the vulnerability, and
    iii. A description of the patch or corrective measure that was implemented to resolve the vulnerability.
d) For any unresolved vulnerability:
    i. An assessment of the significance of the vulnerability, and
    ii. The problem ticket number for the outstanding patch or corrective measure, or

iii. The rationale for not implementing a patch or a corrective measure.

6.7 TRANSITION SERVICES

The Transition Services delivery has been divided in different phases including the On-going support requirement. The Contractor may proposed a more iterative approach for the Design and Configuration phases. The Contractor should provide his delivery approach, LSRMS Team resource(s) requirements and Project Schedule in the Project Management Plan.

6.7.1 **Transition-In Services**

The **LSRMS Solution** must ready for deployment no later than 12 months after Contract Award.

6.7.1.1 Discovery and Functional Requirement Mapping (Product and Solution Roadmap)

The Contractor must provide to the Project Authority within 20 business days after Contract Award a Product and Solution Roadmap which must include a feature list of the ***LSRMS Solution***, as well as a mapping of the ***LSRMS Solution*** to the functional requirements defined in *Part 3 - Functional Requirements*.

After the Discovery and Functional Requirement Review, the Contractor will update the Product and Solution Roadmap with Configuration and Extension requirements for the ***LSRMS Solution*** and provide the final Product and Solution Roadmap within 60 business days after Contract Award.

6.7.1.2 Transition-In Plan

The Contractor must provide to the Project Authority a Transition-In Plan in the Project Management plan schedule for review and acceptance by the Project Authority.

The Transition-In plan must outline how PSPC will transition to the ***LSRMS Solution*** and, include details on:

a) Configuration activities,
b) Data conversion and migration,
c) Training for LSRMS project team on solution capabilities
d) Integration and testing activities,
e) Connectivity with PSPC systems for example SIGMA
f) Discovery research and assessment to determine specific requirements for processing various components of the ***LSRMS***,
g) Testing operational solutions,
h) Delivering functional capability,
i) Enabling TB clients and User onboarding,
j) Onboarding legacy data,
k) Developing solution specific guidelines,
l) Developing operational procedure documentation, and
m) Developing a thorough implementation readiness assessment;
    I. Plan and schedule,
    II. Scorecards and reports,
    III. Identified and defined critical criteria to drive go and no-go decisions (related to overall readiness and preparedness for going live with any new service or IT environment).
    IV. Rollback strategy.

The Contractor must work collaboratively with PSPC in the development of the Transition-In Plan.

The Contractor’s Transition-In Plan must:

a) Take a milestones-based approach to managing transition-in activities given the size and complexity of the activities required to ensure a smooth transition-in. The approach must divide the ***LSRMS*** into functional components that can be implemented and delivered rapidly.
b) Include a high level assessment of PSPC’s current state and identify areas of change, including key policies and business process.

6.7.1.3 Transition-In Delivery (or execution)

The Contractor must:

a) Execute the Transition-In Plan,
b) Identify high risk Transition areas and impact, develop mitigation strategies, and recommended mitigation actions and report results to PSPC,
c) Review and document current state PSPC and generic PSPC processes (based on existing business process documentation and by facilitating workshops) and document gaps between current state and the **LSRMS Solution** provided processes,
d) Make suggestions related to the improvement and re-engineering of existing end-to-end PSPC-wide processes including a proposed business model (or capability model) and a data model,
e) Facilitate workshops to socialize the processes within the **LSRMS Solution** and discuss and analyze the proposed process optimization and re-engineering,
f) Finalize changes and documentation of new business processes required to align to configured environment,
g) Submit to PSPC for acceptance the final documentation of new business processes for the new **LSRMS Solution** environment,
h) Conduct implementation readiness assessments and report findings and recommendations on a weekly interval basis prior to cutover and identify any items or situations that will impede successful cutover;
i) Perform and complete remediation actions based on readiness assessments and report status to PSPC;
j) Verify that all work, testing, evaluation, assessments, and corrective remediation activities are performed and successfully completed to ensure PSPC achieves 100% implementation readiness for all implementation criteria prior to going live,
k) Provide recommendations on best course(s) of actions to take to address and resolve stakeholder issues;
l) Develop a pre-implementation checklist and post-implementation measurable evaluation criteria,
m) Make go/no-go recommendations and prepare an implementation decision document for acceptance,
n) Complete all post-cutover activities per the project plan ensuring 100% completion of post-cutover activities, and
o) Provide status reports and risk mitigation plans periodically.

PSPC may review the Contractor’s interim work products which are produced in the normal course of implementing the **LSRMS Solution**. PSPC will notify the Contractor, within a reasonable time period, when PSPC would like to informally review these Contractor’s interim work products, and provide comments and/or suggestions in a timely manner. PSPC may also require the Contractor to provide any additional information it deems necessary, including the identification, security clearance and qualification of the personnel responsible for specific testing activities.

6.7.1.4 Transition Integration and System Testing

The Contractor must:

a) Provide proposed integration, test strategy and plan to verify functional, performance, security and reliability requirements that are aligned with User roles, profiles and business processes,
b) Recommend integration and testing requirements,
c) Develop, document and maintain integration and testing plan that meets requirements and adheres to defined policies,
d) Conduct all system testing in accordance with the accepted testing strategy and plan, and
e) Provide PSPC with copies and/or summaries of the test results confirming that all such tests have been executed and passed.

6.7.1.5 User Acceptance Testing (UAT)

PSPC will perform UAT on systems modules and integration work, features and functionalities that are the subject of the LSRMS configurations as defined in the SOW or as requested by PSPC. Prior to releasing functional components into production, the Contractor must submit each major and minor release for UAT by PSPC. Prior to submitting the release for testing, the Contractor must have completed all of The ***LSRMS Solution*** testing required with respect to the release.

During the UAT period, the Contractor must:

a) Assist PSPC in defining User acceptance testing (UAT) strategy, test plan, test scenarios, test cases, entry and exit criteria,
b) Assist PSPC in defining the severity categories and turnaround times,
c) Define with PSPC The ***LSRMS Solution***s or tools to be used to create, track and report defects,
d) Provide PSPC with an escalation, support notification and resolution plan,
e) Provide PSPC with a production-like (test) environment and data to execute UATs,
f) Facilitate the collection of User Acceptance Testing results,
g) Analyze the results of the User Acceptance tests as provided by PSPC,
h) Implement corrective action based on the UAT results and PSPC recommendations,
i) Assess and communicate the overall impact and potential risk to system components prior to implementing changes, and
j) On exit provide PSPC with the complete UAT test results and report.

Upon receiving a release, PSPC will promptly perform UAT in accordance with the applicable scenarios and acceptance criteria, and will inform the Contractor of the outcome of such testing. The PSPC reserves the right to determine the final acceptance criteria for each release.

PSPC will give the Contractor written notice of acceptance of a release when, the release has satisfied the acceptance criteria. A release will be deemed to be accepted by PSPC only upon written notice of acceptance. If the resubmitted release does not conform to the acceptance criteria, PSPC may require the Contractor, at no added cost to PSPC, to continue to correct the deficiencies, and to take whatever action is necessary so that the Deployment Deliverable conforms to the acceptance criteria.

When re-submitting a previously rejected deliverable to the Project Authority, the Contractor must produce a written document that provides a high-level description of how the deliverable was modified from its previously submitted state, and how this modification will address the concern documented by PSPC in the rejection document. Emphasis is to be on establishing conformance with the previously unmet requirements noted in the deliverable rejection document.

6.7.1.6 Program Stabilization and Post-transition

The Contractor must support the PSPC following the transition in order to help it achieve a steady state, including;

a) Resolve any stabilization/post-cutover issues identified by PSPC as high priority within 5 calendar days of each cutover,
b) Conduct post-cutover inspection and submit completed post-cutover checklist within 5 business days following each cutover,
c) Resolve any stabilization/post-cutover issues identified by PSPC as non-high priority within 15 business days of each cutover,
d) Conduct a stabilization assessment within 10 business days following each cutover including analysis and recommendation,
e) Complete all stabilization activities within 30 business days following each cutover,
f) Develop necessary stakeholder communications immediately following each cutover,
g) Collect, analyze and report stakeholder feedback issues, comments and or request,
h) Conduct a post-Transition review within 60 business days of each cutover,
i) Provide a Transition-In Lessons Learned Report for Project Authority acceptance no later than 90 business days after each go-live date based on all lessons learned from the execution of the Transition-In Implementation Plan,
j) Incorporate lessons learned into subsequent Transition activities for example, future cutovers, transitions, transition-out planning,
k) Develop necessary stakeholder communications during post-Transition and obtain acceptance from PSPC, and

6.7.1.7 Technology Road Map

The Contractor must provide, on an annual basis throughout the Term of the Contract, a Technology Road Map that will identify upcoming product releases and upgrades over a 2-year period and allow for the alignment of PSPC business processes with the evolution of the ***LSRMS Solution***.

The Contractor must allow a representative of the Project Authority to participate, as an active voting member, on existing TB client or User committees that solicit feedback on ideas for future software development for all application(s) that makes up the ***LSRMS Solution***. In addition, on an annual basis, the Contractor must solicit PSPC for functionality upgrade ideas and provide feedback as to the feasibility, potential timeline and estimated cost for inclusion in the respective Technology Road Map.

6.7.2 On-Going Support Services

6.7.2.1 On-going Support

The Contractor must support effective management of the ***LSRMS Solution*** for the day-to-day operational activities and the production environment in which it operates, including:

a) Providing documented tools and processes to provide the necessary support for its LSRMS;
b) Providing status reports detailing progress and updates to the ongoing support.

Any identified deficiencies in the software (i.e. bugs, functionality which ceases to work as intended, security vulnerabilities, etc.) must be corrected within a mutually agreeable timeframe. In the event that agreement on a timeframe cannot be reached and Canada is forced to remove the solution from service, the application will be considered unavailable for the purpose of the service standard *5.5.4.1 Application Availability.*

6.7.2.2 Releases, Modifications and Updates

The Contractor must submit a document covering the LSRMS's Release and Upgrade Policy to PSPC within 60 business day after Contract Award.

Once ***LSRMS Solution*** is in production, the Contractor must assess the impact of new releases to the LSRMS application(s) on User and system operations and must ensure that Canada has sufficient notice and opportunity to test releases, upgrades, updates major updates and material changes to the LSRMS prior to their release into production. The Contractor must provide support for testing activities to the PSPC when there are releases, upgrades or updates to the LSRMS, including:

a) Maintain software release matrices across development, quality assurance, and production environments and networks,
b) Provide proposed integration and test plan(s),
c) Conduct integration and security testing for all data and networks based on requirements defined in the plan(s) and PSPC policies and procedures,
d) Evaluate all new and upgraded system components and services for compliance with PSPC security rules, regulations and procedures,
e) Conduct User Acceptance Testing for all modifications and updates, and
f) Assess and communicate the overall impact and potential risk to system components.

The Contractor must take corrective action to mitigate the impact of any release that negatively impacts LSRMS operations.

6.7.3 Maintenance

The Contractor must sustain or restore standard operational conditions for the ***LSRMS Solution*** through a range of planned and unplanned maintenance.

PSPC classifies maintenance activities in the following categories:

1. Corrective Maintenance
2. Preventive Maintenance
3. Adaptive Maintenance
4. Perfective Maintenance

The Contractor must continuously maintain and upgrade the ***LSRMS Solution***, including deploying new updates and releases of the commercial-off-the-shelf solution as they become available, for the entire Term of the Contract.

The Contractor is responsible for providing diagnostic tools to monitor the operation of the overall Contractor ***LSRMS Solution***, for monitoring the ***LSRMS Solution***, and for ensuring the ***LSRMS Solution*** performs according to requirements at all times during the product lifecycle which includes: design, development, implementation, deployments, operation, and decommissioning.

The Contractor is responsible for coordination or execution of planned and ad hoc processes and procedures used in the operational and performance monitoring, management, update, and tuning of the ***LSRMS Solution*** and environment.

6.7.4 Transition-Out Services

Prior to the fulfillment of the Contract or prior to the termination of the Contract, as applicable, the Contractor must deliver, enable and support the necessary activities related to transitioning the in-scope LSRMS to the new service provider or solution (either a new Contractor or to an internal PSPC Department).

This includes:

a) Migration of all LSRMS data to PSPC's new service including the information necessary to map the existing LSRMS's data to PSPC's new service;
b) Providing the new service provider with the lessons learned, assets and documentation from the original transition services provided within the scope of this present SOW;
c) Performing and supporting all activities within the future in-scope service transition plan related to Infrastructure Transition, Transition and Migration, Data Conversion and Migration, Transition Integration and Testing, Organization Change Management & Training Support, and Compliance and Regulations for which only the Contractor (exiting) can be either directly responsible for, or that are dependent on the Contractor's (exiting) support to bring to completion.

6.7.4.1 Transition-Out Strategy

The Contractor must provide to the Project Authority a Transition-Out Strategy within 12 months of Contract Award for review and acceptance by the Project Authority. The Transition-Out Strategy must outline how the Contractor's LSRMS is able to successfully transition to either a new Contractor or to an internal PSPC Department or Agency.

The Transition-Out Strategy must include:

a) Project management,
b) Business change management support,
c) Communications and awareness support,
d) Approach to how information related to data structures, metadata, data content, data domains and data-related processes will be transferred,
e) Data conversion, and migration support,
f) Documentation and file support,
g) Proposed knowledge transfer approach,
h) Operations support,
i) User support,
j) Proposed approach to incumbent relations including systems consulting file layouts, data fields, explaining codes along with general consulting to explain specific administrative procedures and practices, which are not proprietary,
k) Incorporate appropriate items captured in the Lessons Learned Report from the transition-in implementation, and
l) The plan must list the scope of termination (which services), timelines, activities, deliverables, dependencies, milestone dates, resource(s) assignments and level of effort, assumptions and the identification of critical dependencies.

6.7.4.2 Transition-Out Plan

Within 3 months of notification of PSPC's intent to transition-out, the Contractor must provide to the Project Authority a draft Transition-Out Plan to transition out any of the ***LSRMS Solution*** to a new service provider or to a new Contractor or to a new PSPC Department.

The Transition-Out Plan must include:

a) Identify risks and issues associated with each work stream, track and provide to PSPC for review and acceptance,
b) Provide a list and details on subcontracts and associated SubContractor relationships,
c) Provide a list of any third-party software covering licenses, version, upgrade status, license and maintenance fees,
d) Provide list of Contractor staff authorised to access PSPC locations,
e) Provide a list of software, scripts, tools or command procedures required by the Contractor to perform the services being terminated,
f) Provide a list of the processes, standards, procedures, manuals and any associated reference material that are employed by the Contractor to provision services being terminated,
g) Provide a list of all in-flight projects and changes scheduled during termination period,
h) Provide a list of existing known errors,
i) Provide a list of open problems pertaining to the services being terminated,
j) Provide a full list of assets wholly owned by PSPC in the possession of the Contractor ,
k) Identify all third party contracts and licences owned or operated by the Contractor into those that are transferable (with associated costs) and those that are not. For those that are not, the Contractor MUST provide an alternative,
l) Plan for removal of all Contractor external interfaces with PSPC systems according to risk and service provisions, and
m) Provide a list of all the Contractor staff that have access to ***LSRMS Solution*** and provide a schedule for these to be removed during the appropriate exit phase.

6.7.4.3 Transition-Out Assets and Documentation

To support PSPC in the Transition-Out phase and when requested by PSPC, the Contractor must provide the following within 30 business days after notification from PSPC's intent to transition-out:

a) Assets (sole use and shared) and asset registers,
b) Asset maintenance history and status,
c) Contractor data and other information (including SubContractor agreements that are required to provision the services),
d) Configuration information,
e) Data stored in Contractor or third party computer environments — including Contractor Managed Service based environments,
f) All databases containing PSPC owned data,
g) Programs and projects (open and closed ones),
h) Knowledge databases,
i) Incident databases,
j) General documentation that should be included:
    i. Organization services design and architecture representations,
    ii. Software related documentation (e.g. User, authorized administrator),
    iii. Updated/recent process and procedure documentation,

iv. Workflow and work instruction documentation,
v. Service management logs - change and incident logs, and
vi. Risk register.

k) Tactical documentation that should be included:
i. Service-level reports,
ii. Service catalogue,
iii. Service delivery plans,
iv. Incident and change register,
v. Change and project calendar,
vi. Current and scheduled project documents,
vii. Release schedules,
viii. Performance and capacity management planning,
ix. Innovation and service creation plans related to the involved services, and
x. Communication plans and all current and scheduled communication documentation (online and offline);

l) Strategic documentation that should be included:
i. Account plans,
ii. Strategic relationship plans,
iii. Road maps for technology and services, and
iv. Enterprise architecture and governance documentation.

6.8 MEETINGS AND REPORTING

6.8.1 Kick-Off Meeting

The Contractor must organize a Kick-Off Meeting with the Project and the Contracting Authorities in the National Capital Region (NCR), within 10 business days of Contract Award.

The purpose of the Kick-Off Meeting, as a minimum will be to:

a) Review the contractual requirements,
b) Review and clarify, if required, the respective roles and responsibilities of the Contracting Authority, the Project Authority and of the Contractor to ensure common understanding,
c) Establish working relationship among the Contractor and LSRMS Team members, and
d) Discuss the Project management plan, schedule that was proposed as part of the Contractor’s bid submission.

The Contractor must prepare and submit the minutes of the meeting within 5 business days to the Project Authority for acceptance. The minutes of the meeting must provide the names of all attendees, a record of discussions and decisions made. Any required changes will be discussed between the Project Authority and the Contractor.

6.8.2 Weekly Status Meeting

The Contractor must organize, schedule and conduct status meetings on a weekly basis with the Project Authority in the NCR throughout the Transition. The focus of these meetings must be to update the Project Authority on key aspects of the LSRMS project, including schedule review and project health.

The Contractor must prepare and submit the minutes of the meeting within 5 business days to the Project Authority for concurrence/acceptance. The minutes of the meeting must provide the names of all attendees, a record of discussions and decisions made. Any required changes will be discussed between the Project Authority and the Contractor.

6.8.3 Monthly Project Progress Report

The Contractor must prepare and present to the Project Authority for review and acceptance a monthly Project Progress Status Report. This report must contain the following information:

a) Overall project status,
b) Status in relation to the project management plan,
c) Accomplishments for the current period,
d) Critical Path Analysis,
e) Re-Scheduled Milestones,
f) Planned Activities for the next period,
g) Statistical volumetric information,
h) A summary of service level performance,
i) A list and a description of major events,
j) Outstanding/Resolved Risk and Issue statuses, and
k) TB client satisfaction survey results.

6.8.4 Strategic Management Semi-Annual Reviews

The Contractor must prepare and present to the Project Authority and PSPC senior executives on a semi-annual basis, a Semi-Annual Review including presentations of all LSRMS components. The Semi-Annual Review must include the following:

a) Project status, including status of key problems,
b) Issues that the LSRMS is currently facing and a proposal on how to address them, and
c) Risk management status.

6.9 DELIVERABLE SUMMARY

SOW Reference	Deliverable	Time Interval
6.3.1 Project Management Plan (PMP)	Project Management Plan	Draft at bid submission Final within 20 business days after Contract Award
6.3.1 Project Management plan	Detailed Project Schedule	Draft at bid submission Updated and included in the PMP for acceptance Weekly update and review at weekly meeting
6.3.1 Project Management Plan	Risk Register	Draft at bid submission Included in the PMP for acceptance after Contract Award Monthly update with Monthly Progress Report

SOW Reference	Deliverable	Time Interval
6.7.1.1 Discovery and Functional Requirement Review	Product and Solution Roadmap	Draft Within 20 business days after Contract Award Final Product and Solution Roadmap to be submitted 60 business days after Contract Award
6.5.4 Technical Architecture Diagrams	Technical Architecture Diagrams	Draft at bid submission. Final submitted for acceptance as per the Project Schedule
6.5.5 Technical Integration Approach	Technical Integration Approach	Draft at bid submission. Final submitted for acceptance as per the Project Schedule
6.12 Data Migration Plan	Data Migration plan	Within 60 days of Contract Award
6.7.1.4 Transition Integration and System Test	System Test Plan and Report	As per the Project Schedule
6.13 Training, Knowledge Transfer and Documentation	Training Plan	Within 45 business days of Contract Award
6.13 Training, Knowledge Transfer and Documentation	Training Modules and User guide	As per the training plan
6.7.1 Transition In Services	LSRMS Solution ready for deployment	12 months after Contract Award
6.4.1 Privacy Management Plan	Privacy Management Plan Privacy Awareness guide	Within 45 business days of Contract Award Within 60 business days of Contract Award
6.4.2 Privacy Management Plan delivery	Privacy Management Plan (Implementation)	Within 30 business days upon request
6.5.2 IT Security Plan	IT Security Plan	Within 45 business days of Contract Award.
6.6.1.1 Security High level Design	Security High Level Design	As per the Security Plan
6.6.1.2 Security Requirement Traceability Matrix	Security Requirement Traceability Matrix	As per the Security Plan
6.6.3.1 Security Installation Verification Plan	Security Installation Verification Plan	As per the Security Plan
6.6.3.2 Security Installation Verification Report	Security Installation Verification Report	As per the Security Plan
6.6.3.3 Security Integration Test Plan	Security Integration Test Plan	As per the Security Plan
6.6.3.4 Security Integration Test Report	Security Integration Test Report	As per the Security Plan
6.6.3.5 Vulnerability Assessment Plan	Vulnerability Assessment Plan	As per the Security Plan

SOW Reference	Deliverable	Time Interval
6.6.3.6 Vulnerability Assessment Report	Vulnerability Assessment Report	As per the Security Plan
6.11.1 Service Continuity	Service Continuity Plan	Draft at bid submission. Final as per the Project Schedule
6.11 Service Continuity and Disaster recovery plan	Recovery Procedures Test Results	Every 6 months
6.11.3 Disaster Recovery Plan	Disaster Recovery Plan	Draft at bid submission Final as per the Project Schedule
6.7.1.7 Technology Road Map	Technology Road Map	Yearly after On-going Support phase begins
6.7.2.2 Releases, Modifications and Updates	Releases, Modifications and Updates Policy	Within 60 business days of Contract Award.
6.7.4.1 Transition-Out Strategy	Transition-Out Strategy	Within 12 months of Contract Award
6.7.4.2 Transition-Out Plan	Transition-Out Plan	Within 3 months of notification of the PSPC's intent to transition-out
6.7.4.3 Transition-Out Assets and Documentation	Transition-Out Assets and Documentation	Within 30 business days after notification from PSPC's intent to transition-out
6.8.3 Monthly Project Progress Report	Monthly Project Progress Report	Monthly
5.4.3.1 Performance Measurement and Reporting	Monthly Service Management Report	Monthly after On-going Support phase begins
6.8.4 Strategic Management Semi-Annual Reviews	Strategic Management Semi-Annual Reviews	Twice a year

6.10 DELIVERABLES ACCEPTANCE FRAMEWORK

6.10.1 Deliverable Acceptance Framework

With the exception of the deployment of the functional and non-functional requirements described in *Part 3 Functional Requirements* and *Part 5 Non-Functional Requirements*, PSPC will use the following Deliverables Acceptance Framework for all of the Contractor's deliverables:

a. Deliverables received by PSPC will be considered draft until accepted by PSPC. If not accepted by PSPC , the PSPC will provide its feedback on the deliverable to the Contractor within 10 business days following receipt;
b. Upon receipt of this feedback by the Contractor , the Contractor and PSPC may agree to jointly review the feedback prior to its incorporation into the Final Deliverable;
c. The Contractor must submit the revised deliverable to the Project Authority within 10 business days of the receipt of PSPC's feedback, or the joint review of the feedback, whichever is later.
d. The Contractor and PSPC may mutually agree to different timelines or an alternate process for given deliverable(s) than the prescribed above.

6.10.2 Acceptance or Rejection of Deliverables

PSPC reserves the right to reject deliverables. At the end of the review period as identified in *6.12.1* the Project Authority will, in writing, either: (1) accept the deliverable; (2) reject the deliverable, identifying reasons for rejection; or (3) continue the acceptance period in accordance with a mutually-agreed time period for continued review.

In the event that PSPC rejects a deliverable, the Contractor must promptly resolve any outstanding issues that are required in order for the deliverable to meet all applicable Acceptance Criteria. The PSPC will cooperate in the Contractor's efforts to resolve any problems, including indicating the reasons for rejection, and will not unreasonably withhold acceptance.

The PSPC will give the Contractor timely written notice of acceptance of a deliverable when the deliverable has satisfied the acceptance criteria. A deliverable will be deemed to be accepted by PSPC only upon written notice of acceptance.

6.10.3 Re-submission of a Rejected Deliverable

When re-submitting a previously rejected deliverable to PSPC, the Contractor must produce a written document that provides a high-level description of how the deliverable was modified from its previously submitted state, and how this modification will address the concern documented by PSPC in the rejection document. Emphasis is to be on establishing conformance with the previously unmet requirements noted in the deliverable rejection document. This is to both provide assurance that PSPC's needs have been met, and to accelerate the Acceptance Period by enabling PSPC to focus on reviewing the modifications made by the Contractor. The Contractor must identify any changes or issues that were not addressed and provide rationale as to why these changes were not included.

6.10.4 Deliverable Submission Process

In order to avoid acceptance delays, inconsistences and contradictions in related Deliverables, the Contractor should take measures to avoid submitting deliverables at the same time, unless stipulated in the Contract. If the Contractor submits multiple deliverables at the same time, outside the stipulated deliverable dates in the Contract, PSPC reserves the right for additional review time and will adjust *6.10.1* accordingly.

6.11 SERVICE CONTINUITY AND DISASTER RECOVERY PLAN

6.11.1 Context

The Contractor must have in place a comprehensive service continuity and disaster recovery plan that outlines and specifies the procedures to be followed with respect to the continued provision of critical services or products in the event of a service disruption, due to natural disasters, terrorism, cyberattacks, facilities or equipment failure, damaged or destroyed. The Contractor shall make such plans and procedures available to Canada for review.

6.11.2 Service Continuity Plan

Service Continuity Planning is a proactive planning process that ensures critical services or products are delivered during a disruption. Critical services or products are those that must be delivered to ensure survival, avoid causing injury, and meet legal or other obligations to Canada.

The Contractor must include the following in the Service Continuity Plan:

a) Policy, purpose, and scope,
b) Goals and objectives,
c) Assumptions,
d) Key roles and responsibilities,
e) Business Impact Analysis (BIA) results,
f) Risk mitigation plans,
g) Offsite data and storage requirements,
h) Back-up strategy and media,
i) Business recovery and continuity strategies,
j) Alternate operating strategies,
k) Supplier vendor readiness,
l) Plan activation and universal response,
m) Communication and notification plan,
n) Training, drills, and exercises,
o) Review and test,
p) Plan maintenance, and
q) Audits.

6.11.3 Disaster Recovery Plan (DRP)

The purpose is to provide a disaster recovery plan is to respond to unplanned incidents that threaten, destroy or severely cripples the ***LSRMS Solution*** operated by the Contractor or SubContractors. The intent is to have a plan in place to restore operations as quickly as possible with minimal disruption and with the latest and most up-to-date data available. It can include damage to; building, infrastructure, hardware, software, data, and personnel.

The Contractor must provide a Disaster Recovery plan that addresses and contains for example the following:

a) Provide disaster recovery policy , overview and scope of the plan,
b) Documents and diagram of the entire network and recovery site,
c) Communication and notification plan,
d) Outline of the triggers used to invoke the plan,
e) A list of the internal and external stakeholders involved in each procedure covered, complete with contact details and a description of the roles and responsibilities,
f) Ready-to-use forms and documents used to help complete the plan,
g) Description of the emergency response, backup operations, recovery actions procedures including the Recovery Point Objective (RPO) and Recovery Time Objective (RTO),
h) A list of software and systems that will be used in the recovery,
i) Identify the most serious threats and vulnerabilities, and the most critical assets to the ***LSRMS Solution***;
j) Summary of insurance coverage,
k) Proposed actions and details for dealing with financial and legal issues, and
l) Description, details, tests reports and schedule on the disaster recovery plan audit.

6.11.4 Requirements

SOW NUM	**Requirement (RATED)**
DIS-RECOV-01	The Contractor should complete a test of the Recovery Procedures every 6 months and provide the results to PSPC.

SOW NUM	Requirement (RATED)
DIS-RECOV-02	The Contractor should maintain, at minimum, the following recovery time objectives and the recovery point objectives for the Contractor or SubContractors Central Server: a) Recovery time objective is 24 hours b) Recovery point within 48 hours.
DIS-RECOV-03	The ***LSRMS Solution*** should protect all PSPC data and logs generated or updated in the solution from any loss.
DIS-RECOV-04	The Contractor should establish the following recovery procedures; a) Backup, b) Disaster recovery, including whole facility failure scenarios, c) Data protection, d) Data retention and disposal, and e) Archiving – online, near line and off line, (collectively the “recovery procedures”).
DIS-RECOV-05	The ***LSRMS Solution*** should ensure that archived information can be restored for full access within 1 business day.
DIS-RECOV-06	The ***LSRMS Solution*** should retain in the archive of the Contractor or SubContractor Central Server all information collected by the ***LSRMS Solution*** including audit logs.
DIS-RECOV-07	The Contractor should ensure ongoing capability for PSPC to be able to recover, without dependency on the Contractor, archived data from media as specified by PSPC.
DIS-RECOV-08	The Contractor should provide emergency procedures, documentation, and training pertaining to handling emergency situations upon request by PSPC.
DIS-RECOV-09	The Contractor should provide problem diagnosis which includes procedures for determining the cause, forecasting the extent, and proceeding with remedial actions for any hardware, or software outage.
DIS-RECOV-10	The Contractor should maintain, document, and support facilities for off-site data storage and retrieval of data from the Contractor or SubContractor central data centre.
DIS-RECOV-11	The Contractor should provide documentation and set of procedures pertaining to the ability to provide contingency recovery at the back-up data centre.
DIS-RECOV-12	The Contractor should provide documentation on how manpower will be obtained and used in the event of a disaster situation.
DIS-RECOV-13	The Contractor should perform periodic testing of the various aspects of the disaster recovery plan as requested by PSPC.
DIS-RECOV-14	The Contractor should provide documentation on how the Contractor or SubContractors Central Server addresses physical security such as; access control, fire prevention and protection, and electrical failure protection.
DIS-RECOV-15	The Contractor should provide the back-up frequency, schedule, sites, and type of media used.
DIS-RECOV-16	In the event that the Contractor intends to change the disaster recovery plan for any reason the Contractor must provide Written notice of its intention fifteen (15) Business Days prior to the implementation date of the Proposed Changes to the Technical Authority.
DIS-RECOV-17	The Contractor should allow PSPC to review and approve the disaster recovery plan and any updates thereafter.

SOW NUM	Requirement (RATED)
DIS-RECOV-18	The Contractor should provide disaster recovery test plan, schedule, and test results to PSPC.
DIS-RECOV-19	The Contractor should provide PSPC with the history of unplanned incidents and outages, and how they were handled.
DIS-RECOV-20	The Contractor should provide PSPC with the past and current disaster recovery plan audit results.

6.12 DATA MIGRATION PLAN

6.12.1 Context

A data migration plan is crucial to ensure that all Bureau resource(s), systems, services, and applications have access to the information assets in the ***LSRMS Solution***. In order to accomplish this, data migration needs to be thoroughly planned and effectively implemented to help ensure the quality and reliability with minimal disruption to the business.

The Contractor must upload the Legacy data in the LSRMS Solution and assist the Bureau in the transfer of data from its legacy system to the ***LSRMS Solution***. The data migration plan provides an outline of four key areas and corresponding sub-area that should be addressed.

6.12.2 Data Migration

The data migration plan consist of four key areas, project planning (scope, risks, constraints), specification (requirements gathering), analysis (inspecting the source data) and implementation (extract, cleansing, transformation, load, test and GO LIVE).

The Data Migration Plan must address and include the following:

Project Planning:

a) Develop data migration project plan,
b) Determine the scope of the migration project,
c) Determine project team and resource(s) ,
d) Define and assign roles & responsibilities,
e) Determine Risks/Constraints/ Dependencies /Assumptions,
f) Develop data migration risk mitigation plan,
g) Determine the timelines, budget and cost,
h) Determine critical success factors,
i) Develop data migration communications plan,
j) Determine the service agreement for the migration, and
k) Determine milestone and Go Live.

Specification:

a) Determine business requirements and expectations,
b) Determine data migration requirements and method,
c) Determine the data extract, cleansing, transformation and load requirements,
d) Determine the conceptual, logical and physical model data requirements for the target, environment based on the source environment models,
e) Determine the data mapping rules and constraints,

f) Determine data mapping requirements,
g) Determine the staging environment capacity, technology and IT infrastructure requirements,
h) Determine the target environment capacity, technology and IT infrastructure requirements,
i) Determine the interface requirements between source, staging and target,
j) Determine the data security and privacy requirements,
k) Determine data remediation and roll-back requirements,
l) Determine the requirements for the data extraction, cleansing, transformation, load and testing scripts, and
m) Determine the data integrity and quality assurance testing requirements.

Analysis:
a) Assess the technology and IT infrastructure of the source environment,
b) Identify the conceptual, logical and physical model of the data in the source environment,
c) Identify the data metadata in the source environment,
d) Assess the quality of the data in the source environment,
e) Identify the source of the data,
f) Identify where the source data is stored, backed up, and archived, and
g) Identify the data usage, capacity, and growth patterns.

Implementation:
a) Set up and configuration of the staging and target environment
b) Data extraction, cleansing and testing
   1. checking the quality of the source data,
   2. remove duplicate data and ensure data matches across the separate sources,
   3. Script creation and testing (database queries and program scripts to extract data into a logical model from source data and to test the data).
c) Data transformation,
d) Data transformation testing,
e) Data load,
f) Data load testing,
g) User acceptance testing,
h) Roll-back, and
i) GO LIVE

6.13 TRAINING, KNOWLEDGE TRANSFER AND DOCUMENTATION

6.13.1 Context

Training, knowledge transfer and supporting documentation will equip PSPC with the information, skills and capabilities needed to transition to the ***LSRMS Solution***, to perform the day to day operation and to provide the necessary expertise to use the features and functionalities of the solution to deliver Translation, Terminology, and Interpretation services to the TB client.

The Contractor must provide the following:

a) To the Project Authority a training plan within 45 business days of Contract Award for review and acceptance by the Project Authority

b) Training for the improvement of skills through education and instruction for Contractor's staff. The Contractor must participate in any initial and ongoing training delivered by PSPC as required that would provide a learning opportunity about PSPC's business and technical environment.

c) Training for the purpose of enabling PSPC’s staff to utilize the features and functions of the ***LSRMS Solution*** and services. Delivery methods may include classroom style, computer based, individual or other appropriate means of instruction.

d) The training environment that includes the ***LSRMS Solution***, components, and documentation necessary to support the training of PSPC staff.

6.13.2 Training and Knowledge Transfer

Training and Knowledge Transfer Services are the activities and deliverables which assure the bi-directional transfer of knowledge between PSPC and the Contractor necessary to enable individuals to complete the work in this SOW.

The following table identifies the training and knowledge transfer activities the Contractor should provide in collaboration with PSPC:

Activity	
a)	Develop the training approach for both pre and post transition which may include coaching approach, train-the-trainer program, onsite, remote classroom-style training, jobs aids, User guides, and step action charts~~.~~
b)	Provide a comprehensive audit of PSPC employee skill-levels, identifying knowledge gaps and recommending the tools, and training required to use and support the ***LSRMS Solution***.
c)	Develop, document and maintain training and knowledge transfer procedures in Canada’s Official Languages that meet requirements and adhere to defined policies.
d)	Support identification of key stakeholders (in conjunction with change management team) and creation of training materials for User acceptance testing in conjunction with technical team.
e)	Develop and deliver training program in Canada’s Official Languages to instruct PSPC personnel on the provision of Contractor Services for example rules of engagement, requesting services.
f)	Develop and implement knowledge transfer procedures to ensure that more than one individual understands key components of the business and technical environment.
g)	Participate in PSPC delivered instruction on the business and technical environment.
h)	Provide ongoing training materials for service desk personnel on PSPC business and technical environments as defined by PSPC.
i)	Training requirements assessment by User type to address the initial training requirement for the LSRMS to “go live” and the ongoing training requirement for new User or refresher training.
j)	Provide training module content in Canada’s Official Languages (quality vetted by the Translation Bureau) that is copyright and royalty free for modification and redistribution by PSPC.
k)	Provide training when substantive (as defined between PSPC and Contractor) technological changes for example when, new systems or functionality are introduced into the ***LSRMS Solution***, in order to facilitate full exploitation of all relevant features and functionalities.
l)	Provide ongoing training materials for service desk personnel on PSPC business and technical environments as defined by PSPC.

Activity
m) Provide facilities for training of PSPC employees.
n) Review and approve the Contractor training and knowledge transfer procedures.
o) Review and approve the Contractor training and knowledge transfer schedule.

6.13.3 Documentation

Documentation services are the activities and deliverables associated with developing, revising, maintaining, reproducing and distributing ***LSRMS Solution*** information to PSPC in hard copy and electronic form.

The following table identifies the general documentation activities the Contractor should provide in collaboration with PSPC:

Activity
a) Recommend documentation requirements and formats.
b) Define documentation requirements, formats and policies.
c) Develop, document, deliver and maintain documentation procedures that meet the requirements and adhere to defined policies.
d) Maintain and update documentation to support solution, system, features and functionalities when new capabilities or changes are introduced.
e) Document standard operating procedures as specified by PSPC for example, boot, failover, batch processing, and backup.
f) Ensure that documentation meets PSPC language quality standard for Canada’s Official Languages.

6.13.4 Requirements

SOW NUM	**Requirement (MANDATORY)**
TRNG-01	The Contractor must provide training to PSPC on the CAT tools which includes for example; analyzer, editor, TM, MT, and QA modules.
TRNG-02	The Contractor must provide training in Canada’s Official Languages.
TRNG-03	Training materials must comply with the approved training plan and available in Canada’s Official Languages.

SOW NUM	**Requirement (RATED)**
TRNG-04	The training environment should include all PSPC workflows and must interoperate with a PSPC managed training environment.
TRNG-05	The Contractor should provide training to PSPC on proper use of audit tools and procedures.
TRNG-06	The Contractor should provide training to PSPC on proper use of analytics, reporting, business intelligence tools and procedures.
TRNG-07	The Contractor should provide training to PSPC on the ***LSRMS Solution*** workflow management features and functionalities.

SOW NUM	Requirement (RATED)
TRNG-08	The Contractor should provide training to PSPC on the ***LSRMS Solution*** workload management features and functionalities.
TRNG-09	The Contractor should provide training to PSPC on the ***LSRMS Solution*** security features and functionalities.
TRNG-10	The Contractor should provide training to PSPC on the ***LSRMS Solution*** portal design, features and functionalities.
TRNG-11	The Contractor should provide training to PSPC on service desk processes and procedures.
TRNG-12	Contractor should provide and update training material as needed or concurrent with a major release to address new features and release changes.
TRNG-13	The Contractor should conduct User training based on the role, access rights, and permission, including training for PSPC retained technical staff for the express purpose of exploiting the functions and features of the ***LSRMS Solution***.
TRNG-14	Delivery methods should include classroom-style, computer-based, webinars, individual or other appropriate means of instruction.
TRNG-15	The Contractor should conduct training for Translators, Terminologist, and Interpreters, external resource(s) (LSPs), and other designated PSPC resource(s).
TRNG-16	The Contractor should conduct User training as requested by PSPC, including selected classroom-style and computer-based training (case-by-case basis) for standard Contractor Hosted Managed Service applications, including new employee training, upgrade classes and specific skills.
TRNG-17	The Contractor should conduct Train the Trainer training for User as defined by PSPC.
TRNG-18	The Contractor should provide role-specific training to Project staff prior to each new product version release in order to facilitate full exploitation of all relevant functions and features of the ***LSRMS Solution***.
TRNG-19	The Contractor should if requested by PSPC, inform and train Users based on the role, access rights, and permission about the end-to-end solution that will support their business requirements.
TRNG-20	The Contractor should provide the training environment to reflect updates and upgrades to the production environment.
TRNG-21	The Contractor should provide the necessary training and knowledge transfer tailored to PSPC User or resource(s) role, access rights and permission.

6.14 CHANGE MANAGEMENT

6.14.1 Context

The purpose of the Change Management is to control the lifecycle of all Translation, Terminology, and Interpretation change requests related to the solution by standardizing the methods and procedures to handle the change, minimize impacts to stakeholders, and disruption to services that could affect PSPC and its TB clients.

Change Management defines different types of changes that may be requested and considered such as; application, hardware, software, network, environmental, documentation, incident and problem changes.

The Contractor must provide consultation, professional services and support to assist PSPC with change management and approach.

6.14.2 Objective

The objectives of the Change Management are to:

a) Respond to the customer’s changing business requirements while maximizing value and reducing incidents, disruption and re-work,
b) Respond to the business and IT Requests for Change (RFC) that will align the services with the business needs and goals,
c) Ensure that changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner,
d) Optimize overall business risk,
    i. It is often correct to minimize business risk, but sometimes it is appropriate to knowingly accept a risk because of the potential benefit.
e) Manage changes to:
    i. Optimize risk exposure (supporting the risk profile required by the business),
    ii. Minimize the severity of any impact and disruption,
    iii. Achieve success at the first attempt, and
    iv. Ensure that all stakeholders receive appropriate and timely communication about change so that they are aware and ready to adopt and support the change.

6.14.3 Approach

This section of Change Management describes the approach PSPC will use for managing the lifecycle of the change. In doing so it will ensure that all proposed changes are defined, evaluated, reviewed, and approved so they can be properly implemented and communicated to all stakeholders.

The following approach and activities must be used as part of Change Management and should be performed by the Contractor in collaboration with PSPC:

1.0 Prepare request for change (RFC)
a) Create and complete the Request for Change (RFC) refer to section *6.14.4 Request for Change (RFC*), for the type of information required for the request for change (RFC)
b) Clarify the objectives and information for the change and evaluate
c) Conduct an analysis to define the risks, cost and specific impact of the change on the stakeholders
d) Review and Signoff (stakeholders, technical, Contractor , executive)
e) Authorize the Change

2.0 Plan the change
a) Stakeholder, technical, and executive sponsor activities
b) Contractor consultation and professional services needed for the change
c) Communications plan
d) Back-out plan and approach
e) Training plan and schedule

3.0 Manage and implement the change
a) Obtain necessary resource(s) and organize to manage the change
b) Test and validate the change

c) Schedule the change
d) Implement the change
e) Invoke back-out plan if required

4.0 Review, document and close the change
a) Post Implementation review
b) Collect feedback to measure results and the adoption of the desired change.
c) Take corrective action to close any gaps
d) Define and implement key performance indicators (KPIs) and measurements.
e) Document the change
f) Close the change

6.14.4 Request for Change (RFC)

The Change Management request for change (RFC) will be used to communicate the change and should contain the following information for example;

RFC Information	
a) Date and time of the change request,	
b) Contact information of the requester,	
c) Change type (standard, normal, emergency;	
i. Standard	Changes to a service or to the IT infrastructure where the implementation process and the risks are known upfront. These changes are managed according to policies that are the IT organization already has in place. Since these changes are subject to established policies and procedures, they are the easiest to prioritize and implement, and often don't require acceptance from a risk management perspective.
ii. Normal	Those that must go through the change process before being accepted and implemented. If they are determined to be high-risk, a change advisory board must decide whether they will be implemented.
iii. Emergency	When an unexpected error or threat occurs, such as when a flaw in the infrastructure, security breach, application malfunction, and incident that needs to be addressed immediately.
d) Change category (critical, major, minor),	
e) Priority,	
f) Description of the change (scope),	
g) Reason for change,	
h) Impacts of the change to: I. Groups or resource(s) , II. Tools (system, application), and III. Features and functionality.	
i) Effect of not implementing the change,	
j) Benefits of applying the change,	

RFC Information
k) Costs of applying the change,
l) Risk assessment of the change, and
m) Implement the change: i. Estimated timeframe, ii. Estimated downtime, iii. Schedule, iv. resource(s) required, and v. Physical location

6.14.5 Delivery

The Contractor should provide Change Management Procedures to PSPC that includes;

a) Work in collaboration with PSPC in executing the Change Management and approach,
b) Contractor 's change management authorities,
c) Contractor resource(s) roles and responsibilities for change management,
d) How the Contractor will use the change management process and established PSPC governance to support the development of the LSRMS,
e) Description of the change management process, including the change review and acceptance l process,
f) Identify high risk areas and impact, develop mitigation strategies, and recommended mitigation actions and report results to PSPC,
g) Facilitate workshops to discuss, review, analyze and validate changes,
a) Conduct readiness assessments and report findings and recommendations,
b) Measures used to enforce only authorized changes,
h) Perform and complete remediation actions based on readiness assessments and report status to PSPC,
i) Provide recommendations on best course(s) of actions to take to address and resolve stakeholder issues;
j) Change Management and issue escalation log, and
k) Provide status reports and risk mitigation plans periodically as required by PSPC.

6.14.6 Requirements

SOW NUM	Requirement (MANDATORY)
CHG-MGMT-01	In the event that the Contractor intends to change its Contractor or 3rd party data center infrastructure or any part thereof that may in any way impact the LSRMS services, it must provide Written notice of its intention fifteen (15) Business Days prior to the implementation date of the proposed changes to the Technical Authority.
CHG-MGMT-02	All potential changes to the Contractor or SubContractor central service infrastructure, or any part thereof, that may in anyway impact the LSRMS services, where the Contractor has provided notice in accordance with requirement CHG-MGMT-04, must be accepted in writing by PSPC prior to implementing the proposed changes.
CHG-MGMT-03	The Proposed Change must describe the proposed changes in sufficient details to permit the Technical Authority to evaluate whether or not the proposed changes would impact PSPC business use and operation of the ***LSRMS Solution***. If PSPC determines that the Proposed Changes may have an impact on its use or operation of the ***LSRMS***

SOW NUM	Requirement (MANDATORY)
	Solution, it shall notify the Contractor in writing of such impact. The Contractor must make the required modifications to the proposed changes, in order to ensure that they do not impact the use or operation of the ***LSRMS Solution***.
CHG-MGMT-04	The Contractor must not implement the proposed changes or the modified proposed changes until acceptance is obtained from the Technical Authority.
CHG-MGMT-05	Regardless of the acceptance of the proposed changes by PSPC, the Contractor must comply with its obligations set-out in this SOW.
CHG-MGMT-06	The Contractor must implement a product development life cycle which provides auditable change management which identifies with each product version, the set of enhancements, corrected deficiencies, known issues, and accepted versions of supporting hardware, operating system, training, maintenance and other materials to be used with the release.
CHG-MGMT-07	For every release of the ***LSRMS Solution*** submitted to PSPC by the Contractor for testing, the Contractor must include a release document which fully describes the configuration of the release and include for example; a) Release description; b) The list of Requests for Change implemented; c) The list of Task Authorizations implemented; d) The list of known bugs; e) The version of each ***LSRMS Solution*** component comprising the release, including all documents (designs, specifications, manuals, and training materials). f) Release testing notes identifying the details of the testing that the Contractor has completed.

SOW NUM	Requirement (RATED)
CHG-MGMT-08	The ***LSRMS Solution*** should implement a product development life cycle which provides an auditable record of deficiencies, corrective actions, testing and verification of deficiency resolution.
CHG-MGMT-09	The Contractor should manage changes and corrective actions in relation to all Solution components
CHG-MGMT-10	The Contractor should assess the risks associated with any changes and corrective actions in relation to the ***LSRMS Solution*** and for sharing all details with PSPC.

6.15 RELEASE MANAGEMENT

6.15.1 Context

Release management Services are activities and deliverables related to implementing changes to services and covers software, hardware and supporting documentation such as specifications, policies, procedures and training material.

Release management Services take a comprehensive view of a change to a service to ensure that the technical and non-technical aspects of a release are integrated and meet all requirements.

These changes can be implemented by rolling out a combination of new applications or infrastructure software and/or upgraded or new hardware, or simply by making changes to the documentation.

Release management processes and activities are inter-related and complementary with the change management process, as well as incident management and problem management.

6.15.2 Release Management

The following table identifies the release management activities the Contractor should provide in collaboration with PSPC:

Activity
a) Participate in the development of the release management process, policies and procedures in collaboration with PSPC.
b) Document and deliver release management policies, procedures, processes, and training requirements per the release management process.
c) Provide release management process, procedures and policies to PSPC for review and acceptance.
d) Establish, manage, update, and maintain the overall release management process, policies, procedures and release schedule for all planned releases.
e) Develop, manage, update and maintain the overall release management process, policies, procedures and release schedule for each release in coordination with Change Management.
f) Establish and administer version control as it relates to release management of PSPC applications.
g) Provide release management process, policies, procedures and release schedules to PSPC for review and acceptance.
h) Develop quality plans and back out plans as appropriate for each release to PSPC for review and acceptance.
i) Conduct site surveys, as necessary, to assess existing equipment and software being used to validate release package requirements and dependencies.
j) Provide resource(s) levels and requirements for supporting a release.
k) Ensure that any new software, equipment, or support services required for the release are procured and available when needed.
l) Ensure that all necessary testing environments are available and properly configured to support release testing.
m) Schedule and conduct release management meetings to include review of planned releases and results of changes made.
n) Review release management details and alter as appropriate to meet the needs of PSPC such as, back out plan, and go/no go decision.
o) Provide release documentation as required.
p) Notify PSPC of release timing and impact and provide communications to the service desk.
q) Implement release in compliance with change management requirements.

Activity
r) Conduct post mortem of releases that necessitated implementation of the back-out plan and develop and implement appropriate corrective or follow up actions to minimize future occurrences.
s) Review and accept input to PSPC User training and communication materials.
t) Plan and manage the User acceptance testing process for each release.
u) Review and accept release UAT process and schedule.
v) Provide PSPC release management reports for each release which include: i. The latest version of each component and software comprising the release ii. Component and software version compatibility requirements iii. The list of RFCs included in the release iv. The list of outstanding RFCs, known issues, and when available work arounds v. UAT reports of all testing activities.
w) Perform quality control audits and accept release control results.

7 PROFESSIONAL SERVICES

7.1 PROFESSIONAL SERVICES

The work described in this section will be requested by PSPC through a Task Authorization on an as and when requested basis.

7.1.1 Additional Change Management and Business Transition Support Services

In addition to the services described in *Section 6.7 Transition Services*, the Contractor must, on an as and when requested basis, provide additional services.

Professional Services Categories
For work described in accordance with *7.2.1 Additional System Configuration, Section 7.2.2 Legacy Data Migration, Section 7.2.3 Third Party Integration,* and *Section 7.2.4 Access to Data of this annex.*

The Contractor may be called upon to provide the professional services outlined below on an as and when requested basis, during the entire Term of the Contract, including any extensions to it exercised as options by the Contracting Authority refer to *Appendix D - Professional Service* resource(*s) responsibilities;*

a) Project Manager
b) System Analyst
c) Data Conversion Specialist
d) Business Analyst
e) Business Process Re-engineering (BPR) Consultant
f) Network Security Analyst.

7.2 ADDITIONAL WORK

The work described in this section will be requested by PSPC through a Task Authorization on an as and when requested basis.

7.2.1 Additional System Configuration

In accordance with *Part 5 Non-Functional Requirements*, PSPC anticipates that there may be a need to modify the solution to accommodate changes in the operational environment. While the Statement of Work clearly defines a flexible solution that can be configured by Translation Bureau resource(s), PSPC may request additional services in support of changes to the ***LSRMS Solution*** configuration.

The Contractor must provide additional services and must propose resource(s) that are qualified and have experience providing Additional System Configuration for the provision of the services.

The Contractor may be called upon to provide Additional System Configuration services, on an as and when requested basis, to assist in the analysis, design, development, configuration, testing, and roll out of system configurations to the baseline ***LSRMS Solution***, including for example the following:

a) Service request management;
b) Portals (TB client, internal and external - templates and forms);
c) Workflow management (Tasks, business rules, validation)
d) Workload management (resource(s) profiles, roles, planning, scheduling, dispatching);

e) CAT (Translation Memory, TermBase, Machine Translation)
f) Business Intelligence, dashboards and reports;
g) System Fields; and
h) Localization and Branding.

7.2.2 Legacy Data Migration

The Contractor must provide Legacy Data Migration services and must provide experienced resource(s) to perform Legacy Data Migration for the provision of the services.

In accordance with *Section 4.4 LSRMS Technology Requirements*, the Contractor must deliver, enable and support data migration from existing PSPC legacy systems and transitional data feeds not already articulated in the Statement of Work, on an as and when requested basis.

7.2.3 Third Party Integration

The Contractor must provide 3rd Party Integration and must provide resource(s) that are qualified and have experience providing 3rd Party Integration for the provision of the services.

In accordance with *Part 4 Technical Requirements*, the Contractor must deliver, enable and support integration with additional 3rd Party systems and data feeds not already articulated in the Statement of Work, on an as requested basis.

7.2.4 Access to Data

On an as when requested basis, the Contractor must provide a copy of PSPC's ***LSRMS Solution*** data in a manner to be defined by PSPC. The copy of data will reside in Canada. Requirements such as types of data, security requirements, file format, frequency of delta updates and the location of data storage will be determined at a later date. The format of the data must remain in its native format and must not be converted to a proprietary format as Canada must have the ability to access its data at any time.

8 APPENDIX A – GLOSSARY OF TERMS

GLOSSARY OF TERMS

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

Acceptance Test: A test of a system or functional unit performed by the **Client** on their site after installation with the participation of the Contractor to ensure that the contractual requirements are met.

Access Control: Security Controls that support the ability to permit or deny access to resource(s) within the LSRMS.

Access Right(s): An approach to control, regulate or restrict system access to a User according to the User's assigned role(s) and rights.

Actual Uptime: The actual time that a service is operational without disruption.

After-Hours Emergency Service (AHES): The AHES is responsible for providing emergency linguistic services after 5 p.m. during the week, and on weekends and statutory holidays.

Analysis: Is the term commonly used in businesses to describe a product (analytical report, statistical analysis or model, or other report or summary of data) produced specifically to answer a single, business question.

Analytics: Analytics often involves studying past historical data to research potential trends, to analyze the effects of certain decisions or events, or to evaluate the performance of a given tool, resource(s), Task or *activity*. The objective of analytics is to improve the business by gaining knowledge which can be used to make improvements or changes.

Annex: An annex can stand alone, it offers additional information than contained in the main document

Appendix: Contains data that cannot be placed in the main document and has references in the original copy or file.

Application Availability: The percentage of time the ***LSRMS Solution*** is available for normal business operations.

Application Programming Interface (API): An API is a set of routines, protocols, and tools for building applications, including interfaces that allow software and hardware components to communicate with each other.

Approver: Is a role assigned, on a case by case basis, to define an additional level of acceptance throughout the acceptance process.

Audit and Accountability (AU): Security controls that support the ability to collect, analyze, and store audit records associated with User operations performed within the information system.

Audit: An examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives.

Authentication: Process to verify the digital identity of the sender of a network communication.

Automated Attendant (AA): Includes a series of recorded messages describing actions that a caller can take to access particular services. An auto-attendant can route multiple simultaneous phone calls to the appropriate person.

Availability: Network, Storage, Server, SLA - min 99.95. This metric is the percentage of time that a service or system is available. It is the ratio of time a system or component is functional to the total time it is required or expected to function. This can be expressed as a direct proportion (for example, 9/10 or 0.9) or as a percentage (for example, 90%). It can also be expressed in terms of average downtime per week, month or year or as total downtime for a given week, month or year. Sometimes availability is expressed in qualitative terms, indicating the extent to which a system can continue to work when a significant component or set of components goes down.

B

Broadcasting Premiums: In agreement with TR collective agreement:

a) **Parliamentary Interpreters:** A supplement of five dollars and fifty cents ($5.50) for each gross hour of interpretation shall be paid to an employee who interprets the debates of the House of Commons. This supplement shall be paid twice (2) each fiscal year. For this purpose, total interpretation time shall be calculated daily to the nearest quarter (1/4) hour.

b) **Conference interpreters:** A supplement of seven dollars ($7) for each gross hour of interpretation shall be paid to an employee interpreting a debate or conference that is broadcast live. This supplement shall be paid twice (2) each fiscal year. For that purpose, the total interpretation time during a live broadcast shall be calculated to the nearest quarter (1/4) hour.

Business Day: Is any working day, Monday to Friday inclusive, excluding statutory and other holidays, and any other day which has been elected by the GC to be closed for business.

Business Impact Analysis (BIA): An analysis that determines the impacts of disruptions on an organization and that identifies and prioritizes critical services and business operations to be maintained.

Business Intelligence (BI): The set of techniques and tools for the transformation of raw data into meaningful and useful information for business analysis purposes.

Business Number: A unique identifying number that is given to a registered business by the Canada Revenue Agency.

c

Central Processing Unit (CPU): Is the electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output operations specified by the instructions.

Change Advisory Board (CAB): A formally constituted group of people representing service delivery and support functions that is responsible for assessing, planning, and authorizing changes to the IT environment.

Change Management: Is a process designed to help control the life cycle of strategic, tactical, and operational changes to IT services through standardized procedures, with the goal to control risk and minimize disruption to associated IT services and business operations.

Client: PSPC's Translation Bureau.

Comma Separated Value (CSV): Is a simple file format used to store tabular data, such as a spreadsheet or database. Files in the CSV format can be imported to and exported from programs that store data in tables, such as Microsoft Excel.

Commercial Off The Shelf (COTS): Describes software and/or hardware products that are ready-made and available as is and not requiring custom development before installation.

Committee on Conformity Assessment (CASCO): CASCO is the ISO committee that works on issues relating to conformity assessment. CASCO develops policy and publishes standards related to conformity assessment, it does not perform conformity assessment activities.

Common Event Format (CEF): The CEF is an open log management standard that improves the interoperability of security-related information from different security and network devices and applications. CEF enables customers to use a common event log format so that data can easily be collected and aggregated for analysis by an enterprise management system.

Communications Security Establishment (CSE): CSE is mandated to acquire and provide foreign signals intelligence, and to provide advice, guidance and services to help ensure the protection of Government of Canada electronic information and information infrastructures.

Computer Aided Translation (CAT): Is a form of language translation in which a human translator uses computer hardware to support and facilitate the translation process.

Concordancer: Is a computer program that automatically constructs a concordance. The output of a concordancer may serve as input to a translation memory system for computer-assisted translation (CAT), or as an early step in machine translation (MT). Concordancers are also used in corpus linguistics to retrieve alphabetically or otherwise sorted lists of linguistic data from the corpus in question, which the corpus linguist then analyzes.

Configurable: Settings that can be modified, out-of-the-box without having to customize, to meet the GC services standards and requirements including IT architecture, functional, performance, availability, maintainability, security, Business Continuity, and Disaster Recovery.

Connectivity: Means devices communicating – then making it possible to transport or receive data. However, this system is more focussed on collecting information than integrating it.

Content Management System (CMS): Is a computer application that supports the creation and modification of digital content. It typically supports multiple Users in a collaborative environment.
Most CMSs include Web-based publishing, format management, history editing and version control, indexing, search, and retrieval.

Contract Award: The method used during a procurement process in order to evaluate the proposals (bidder offers) taking part and award the relevant contract. Usually at this stage the eligibility of the proposals has been concluded and it remains to choose the most preferable among the proposed.

Contract Work Breakdown Structure (CWBS): The term contract work breakdown structure refers to the specific portion of the work breakdown structure that has been associated with a specific project that has been developed and is currently being maintained by the seller in is process of attempting to deliver a subproject or project component to the buyer.**Converted Hours:** Hours of interpretation, converted in accordance with coefficient provided in TR collective agreement (applies to internal staff only, per day, per week, per month, per interpreter.

Corpus (Corpora - plural): Is a collection of texts of written (or spoken) language presented in electronic form. it provides the evidence of how language is used in real situations.

Credentials: Are given to authenticate a User and allow them to access particular systems, features and functionalities. They can be User Id and password pair, bio-metric system, User Id and password associated with one time password, and User Id and password associated with some personal questions only the User can answer.

Credentials Management: Gathering, tracking (e.g., missing or expiring documents), amalgamating and storing evidence (e.g., certifications, legal documents, quality assessments, facility and/or individual security clearances, product test results, statements of service integrity and testimonial material) regarding the current capability and experience of a Supplier. In most cases, Supplier credentials are provided by the Supplier in a bid.

Cryptographic Algorithm Validation Program (CAVP): The Cryptographic Algorithm Validation Program (CAVP) provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components. Cryptographic algorithm validation is a prerequisite of cryptographic module validation.

Cryptographic Module Validation Program (CMVP): Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-1, *Security Requirements for Cryptographic Modules*, and other FIPS cryptography based standards. FIPS 140-2 (link is external), *Security Requirements for Cryptographic Modules*, was released on May 25, 2001 and supersedes FIPS 140-1.

Cutover: The switchover from an old system (hardware and/or software) to a new one. Cutover is the point at which a new system becomes operational.

D

Dashboard: An easy-to-read, Near Real-Time interface that displays the current status (snapshot) of specific information.

Data Architecture: Is composed of models, policies, rules or standards that govern which data is collected, and how it is stored, arranged, integrated, and put to use in data systems and in organizations.

Data Center: A facility used to house computer systems and associated components, such as telecommunications and storage systems.

Data Center Tier 1 - Single non-redundant distribution path serving the IT equipment Non-redundant capacity components Basic site infrastructure with expected availability of 99.671%. Utilized by small businesses and feature: 99.671% Uptime, no redundancy, 28.8 Hours of downtime per year.

Data Center Tier 2 - Meets or exceeds all Tier I requirements Redundant site infrastructure capacity components with expected availability of 99.741%. Partial redundancy in power and cooling, 22 hours of downtime per year.

Data Center Tier 3 - Meets or exceeds all Tier I and Tier II requirements Multiple independent distribution paths serving the IT equipment All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture Concurrently maintainable site infrastructure with expected availability of 99.982%. Utilized by larger businesses and features, no more than 1.6 hours of downtime per year, N+1 fault tolerant providing at least 72 hour power outage protection.

Data Center Tier 4 - Meets or exceeds all Tier I, Tier II and Tier III requirements All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems Fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995%. Serve enterprise corporations and provide the following: 2N+1 fully redundant infrastructure (the main difference between tier3 and tier 4 data centers), 96 hour power outage protection, 26.3 minutes of annual downtime.

Data Model: Organizes data elements (qualitative or quantitative) and standardizes how the data elements relate to one another. A Data Model explicitly determines the structure of data.

Data Visualization: A method of putting data in a visual or a pictorial context as a way to communicate information clearly and efficiently to Users (e.g., a map is a way to visualize which areas of the country get the most rainfall).

Data Warehouse: A system used for reporting and data analysis. Data Warehouses are central repositories of integrated data from one or more disparate sources. They store current and historical data and are used for creating analytical reports for knowledge workers throughout the enterprise.

Delegate: Any person who is granted authorization to act on behalf of another User to perform or approve a defined set of Tasks.

Digital Signature: The cryptographic transformation, which when added to a message, transaction, or record, allows the recipient to verify the signer and whether the initial information has been altered or the signature forged since the transformation was made.

Disaster Recovery Plan (DRP): Is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is a comprehensive statement of consistent actions to be taken before, during and after a disaster. The disaster could be natural, environmental or man-made. Man-made disasters could be intentional (for example, an act of a terrorist) or unintentional (that is, accidental, such as the breakage of a man-made dam).

Document (DOC): Document, or an ASCII text file with text formatting codes in with the text; used by many word processors

Document Management: Is the coordination and control of the flow (storage, retrieval, processing, printing, routing, and distribution) of electronic and paper documents in a secure and efficient manner, to ensure that they are accessible to authorized personnel as and when required.

E

Editor: The editor is the ***LSRMS Solution*** frontend that translators use to open a source file for translation, and query the memory and terminology databases for relevant data. It is also the workspace in which translators can write their own translations if no matches are found, and the interface for sending finished sentence pairs to the translation memory and terminology pairs to the term base.

F

Federal Information Processing Standards (FIPS): Set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government Contractor s and vendors who work with the agencies.

Federal Risk and Authorization Management Program (FedRAMP): Provides a standardized approach to security assessment, authorization, and continuous monitoring of cloud based services.

Federated Identity Management: Allows applications to securely share identity information across multiple domains. In simple terms, it means your Users only ever have to log into one place – your internally hosted identity provider, and all of your applications in any location can trust the information that your identity provider asserts about your Users.

File Transfer Protocol (FTP): Is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

First Point of Contact (FPOC): The service desk or support center is the first tier (point of contact) used for basic issues, such as password resets, use of features and functionalities and basic computer troubleshooting.

Freelancer: A person who works as a translator or interpreter, selling work or services by the hour, day, job, etc.

Fuzzy: Text retrieval technique based on finding matches even when keywords are misspelled or only hint of a concept.

G

Graphical User **Interface** (**GUI):** Is a type of User interface that allows Users to interact with electronic devices through graphical icons and visual indicators.

Government of Canada (GC): Is the federal administration of Canada.

H

Help offered / Help received: Calculated number of interpreter-days. PIS interpreters are sometimes assigned to CIS and vice-versa. This report is necessary for budgetary considerations and production reports.

Host: Means any Internet Protocol (IP) addressable entity connected to an IP-based network.

Hours of paid travel time: Number of hours where an interpreted was paid to travel (without any conversion or coefficient) per day, per week, per month, per TB client, per interpreter, per region, per language, etc.

HyperText Markup Language (HTML): Is the standard markup language for creating web pages and web applications.

HyperText Transfer Protocol Secure (HTTPS): HTTPS is HTTP (HyperText Transfer Protocol)-within-SSL/TLS. SSL (TLS) establishes a secured, bidirectional tunnel for arbitrary binary data between two hosts. HTTP is a protocol for sending requests and receiving answers, each request and answer consisting of detailed headers and (possibly) some content. HTTP is meant to run over a bidirectional tunnel for arbitrary binary data; when that tunnel is an SSL/TLS connection, then the whole is called "HTTPS".

I

Identification (ID): Is the ability to identify uniquely a User of a system or an application that is running in the system.

Incident: Is any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service.

Incident Management: Is a process for logging, recording and resolving incident(s). The aim of incident management is to restore the service to the customer as quickly as possible rather than through trying to find a permanent solution.

Incident Response (IR): Is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach. Incident response (IR) plans are designed to test your company's ability to respond to a security **incident**. The ultimate goal is to handle the situation so that it limits the damage to the business while reducing recovery time and costs.

Indexing: Is a data structure that improves the speed of data retrieval operations on a database table at the cost of additional writes and storage space to maintain the index data structure. Indexes are used to quickly locate data without having to search every row in a database table every time a database table is accessed. Indexes can be created using one or more columns of a database table, providing the basis for both rapid random lookups and efficient access of ordered records.

Information Management (IM) Architect: Provides guidance on information management practice and data architecture and is responsible for the preparation and maintenance of enterprise data models. The IM Architect provides support to business and ITS by analyzing and problem solving data related topics including, but not limited to, data modeling and design, integration, master data management, meta data management, data relationships, data quality, data transformation, and data replication, in addition to data security/privacy.

Information Protection Centre (IPC): Is the GC's point of contact for security incidents.

Information Technology (IT): Is the use of computers to store, retrieve, transmit, and manipulate data, or information, often in the context of a business or other enterprise. IT is considered to be a subset of information and communications technology.

Information Technology Infrastructure Library (ITIL): Is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage.

Information Technology Service Management (ITSM): IT service management (ITSM) refers to the entirety of activities – directed by policies, organized and structured in processes and supporting procedures – that are performed by an organization to design, plan, deliver, operate and control information technology (IT) services offered to customers and include but not limited to IT service support such as;

a) Change management – Standardized methods for effective management of business changes
b) Configuration management – Logical and physical aspects of IT infrastructure plus other IT services
c) Incident Management – Day to day functioning / controls that helps restore acceptable norms of IT practices
d) Release Management – Verification, testing and simultaneous release of IT environment changes

e) Problem Management – Diagnosis of incidents to proactively manage and eliminate errors
f) Service Desk – Facilitates a central interaction platform for the business and customers

Integration: The process of bringing together the component subsystems into one system and ensuring that the subsystems function together as a system. Arrangement of an organization's information systems in way that allows them to communicate efficiently and effectively and brings together related parts into a single system.

Interface: The exchange can be between software, computer hardware, peripheral devices, humans and combinations of these.

International Electro-technical Commission (IEC): Is an international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as electrotechnology.

International Organization for Standardization (ISO): Is an international standard-setting body composed of representatives from various national standards organizations.

Internet Explorer (IE): Is a Microsoft web browser.

Interoperability: The ability for different systems and applications to communicate, exchange data, and use the information that has been exchanged.

Interpreter: A person who interprets, especially one who translates speech orally.

Interpreter-Days: Official measure used in the interpretation field internationally. An Interpreter-Day is recorded every day where at least one Task of interpretation is assigned to an interpreter (regardless of duration), per day, per week, per month, per TB client, per interpreter, per region, per language.

J

JavaSript Object Notation (JSON): Open-standard file format that uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types.

K

Key Performance Indicator (KPI): A type of performance measurement used to measure the success of a particular activity.

Knowledge Base: A repository for performing Knowledge Management that provides the means to collect, organize, retrieve and share current or historical information. The Knowledge Base provides the insight, rationale and/or justification for making an informed decision.

Knowledge Management: Knowledge Management is the process which institutionalizes best practices, training materials, and organizational policies for quick and easy access.

L

Latency (milliseconds): This metric shows the time interval between submitting a packet and arrival at its destination.

Lightweight Directory Access Protocol (LDAP): Is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network.

Linguistic Services Request Management System (LSRMS): Is a type of software for automating many parts of the human language translation process and maximizing translator efficiency includes:

> Translator tool – The translation interface that translators, editors, and others use to create the translations.
>
> Terminology management tool – A tool that enables you to create, save, and manage databases of specific terms relevant to your business.

Load Balancing: A device that acts as a reverse proxy and distributes network or application traffic across a number of servers. Load balancers are used to increase capacity (concurrent Users) and reliability of applications

Localization (I10n): Is a Task that involves the translation and adaptation of a Web page, software application or other product to a particular linguistic and cultural community.

Localization Industry Standards Association Quality Assurance (LISA QA): Was a Swiss-based trade body concerning the translation of computer software into multiple natural languages, which existed from 1990 to February 2011.

M

Machine Translation (MT): A tool that automatically translates content without human intervention.

Metadata: Data that defines and describes other data and it is used to aid the identification, description, location or use of information systems, resource(s) and elements.

Metrics: Measures of performance that observe progress and evaluate trends within an organization.

Microsoft Excel Spreadsheet (XLS, XLSX): Microsoft applications that is used for storing, organizing and manipulating data.

Microsoft Office (MS Office): Suite of Microsoft applications such as Word, Excel, Power Point, and others.

Multilingual Premiums: In agreement with TR collective agreement:

> A supplement of sixty dollars ($60) shall be added to the pay of an employee who occupies an official languages interpreter position for each day during which, at the Employer’s discretion, he performs foreign language interpretation, regardless of the type or duration of such interpretation. This supplement shall be paid annually after the end of the fiscal year.

N

National Institute of Standards and Technology (NIST): Is a metrology laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness

New Release: A system release, a version release, and interim release of licensed software, regardless of whether the Contractor refers to it as a "new release".

Notice: An electronic advertisement that solicits goods or services, indicates that a Solicitation is being updated or changed, or announces a Contract Award.

Notification: A system generated message informing a User of an action required (e.g. approve, deny) or that an action has been completed that requires attention.

Number of Contractor **s and rates:** (average rate, highest rate, lowest rate). Rates are per day for conference and parliamentary interpretation and per hour for visual interpretation. Rates can also exceptionally be quoted per assignment in particular cases.

Number of events by priority: Event are classified by priority A, B or C according to various factors (type of meeting, participants, etc.).

O

Office of the Privacy Commissioner of Canada (OPC): Provides advice and information for individuals about protecting personal information. They also enforce two federal privacy laws that set out the rules for how federal government institutions and certain businesses must handle personal information.

Office Open XML: Also informally known as OOXML or Microsoft Open XML (MOX) is a zipped, XML-based file format developed by Microsoft for representing spreadsheets, charts, presentations and word processing documents.

On-line Analytical Processing (OLAP): Is characterized by relatively low volume of transactions. Queries are often very complex and involve aggregations. For OLAP systems a response time is an effectiveness measure. OLAP applications are widely used by Data Mining techniques. In OLAP database there is aggregated, historical data, stored in multi-dimensional schemas (usually star schema).

On-line Transaction Processing (OLTP): Is characterized by a large number of short on-line transactions (INSERT, UPDATE, DELETE). The main emphasis for OLTP systems is put on very fast query processing, maintaining data integrity in multi-access environments and an effectiveness measured by number of transactions per second. In OLTP database there is detailed and current data, and schema used to store transactional databases is the entity model (usually 3NF).

Open Document Text (ODT): File extension is an OpenDocument Text Document file. These files are most often created by the free OpenOffice Writer word processor program. ODT files are similar to the popular DOCX file format used with Microsoft Word.

Operating System (OS): Is system software that manages computer hardware and software resource(s) and provides common services for computer programs.

Order: A purchase issued against a Method of Supply in accordance with the applicable terms and conditions.

Original Equipment Manufacturer (OEM): Is short for original equipment manufacturer, which is a somewhat misleading term used to describe a company that has a special relationship with computer and IT producers. OEMs are manufacturers who resell another company's product under their own name and branding.

P

Personal Information Protection and Electronic Documents Act (PIPEDA): (the **Act**) Is a Canadian **law** relating to data privacy. It governs how private sector organizations collect, use and disclose **personal information** in the course of commercial business.

Platform: General purpose information systems components used to process and store electronic data, such as desktop computers, servers, network devices, and mobile devices. Platforms usually contain server hardware, storage hardware, utility hardware, software and operating systems.

Portable Document Format (PDF): Is a file format developed in the 1990s to present documents, including text formatting and images, in a manner independent of application software, hardware, and operating systems.

Portal: A specially designed web page which brings information together from diverse sources in a uniform way. Usually, each information source gets its dedicated area on the page for displaying information; often, the User can configure which ones to display. Variants of portals include intranet "dashboards" for executives and managers.

Problem Management: Standardized methods and procedures to minimize the impact of problems.

Process Management: The ensemble of activities of planning and monitoring the performance of a business process. It is the application of knowledge, skills, tools, techniques and systems to define, visualize, measure, control, report and improve processes.

Process Mapping: A process map depicts and models business processes that are performed by Users, roles or actors in an enterprise.

Procurement Process: This process addresses the acquisition of goods and services from requisition to payment.

Production System: Real-time and real-data computer systems that are running in production environment used within GC that will interoperate, communicate, execute programs or transfer data with TMS in order to process GC procurement daily work and to accommodate the activities associated with the execution of one or more Systems in a manner that is fully exposed, made available to and supported for final and intended Users of such Systems.

Project Management Body of Knowledge (PMBOK): This refers to the entire collection of processes, best practices, terminologies, and guidelines that are accepted as standards within the project management industry.

PRojects IN Controlled Environments (PRINCE2): Is a process-based approach to project management and is used primarily in IT paradigms. PRINCE2 is used for many types of projects and may be applied during any stage of project management.

Protected Information: This refers to specific provisions of the Access to Information Act and the Privacy Act and applies to sensitive personal, private, and business information. 1) Protected A (low-sensitive): Applies to information that, if compromised, could reasonably be expected to cause injury outside the National Interest, e.g., disclosure of exact salary figures. 2) Protected B (particularly sensitive): applies to information that, if compromised, could reasonably be expected to cause serious injury outside the National Interest, e.g., loss of reputation or competitive advantage. 3) Protected C (extremely sensitive): applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the National Interest, e.g., loss of life.

Protocol: The special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.

Public-Key Infrastructure (PKI) Entrust: A comprehensive system required to provide public-key encryption and digital signature services across a wide variety of applications. An organization establishes and maintains a trustworthy networking environment by managing keys and certificates through a PKI.

Public Services and Procurement Canada (PSPC): Is the department of the Government of Canada with responsibility for the government's internal servicing and administration. The Minister of Public Services and Procurement.

Q

Quality Assurance (QA): A system of activities whose purpose is to provide assurance that the quality control is in fact being done effectively. For a specific product or service, this involves verification, audits and the evaluation of the quality factors that affect the specification, production, inspection and distribution.

Quality Control: A range of activities, to ensure and verify that the specific quality of the product or service has been met.

R

Real-Time: Data that is active and is at the given point in time being worked on in the LSRMS.

Really Simple Syndication (RSS): Is a type of web feed which allows Users to access updates to online content in a standardized, computer-readable format. These feeds can, for example, allow a User to keep track of many different websites in a single news aggregator.

Record: Information in any format created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Recovery Point Objective (RPO): Is about how much data you can afford to lose before it impacts business operations. Example consider RPO as the moment a User saves a document they are working on, and if The ***LSRMS Solution*** were to crash and the progress is lost, how much of the work is the User willing to lose before it affects them?

Recovery Time Objective (RTO): Is related to downtime and represents how long it takes to restore from the incident (disruption) until normal operations are available to Users. Example below of RTO and RPO;

Tier-1: Mission-critical applications that require an RTPO of less than 15 minutes
Tier-2: Business-critical applications that require RTO of 2 hours and RPO of 4 hours
Tier-3: Non-critical applications that require RTO of 4 hours and RPO of 24 hours

Release Management: Standardized methods and procedures for the integration and flow of development, testing, deployment, and support of the LSRMS.

Reliability: The measures expressed of the ability of a product to function successfully when required, for the period required, in the specified environment.

Remote Access: Access to the LSRMS through an external network (e.g. the Internet).

Reporting: The generation of standard, custom or ad hoc reports, based on specific fields of required information that are displayed in the most suitable format.

Repository: An electronic location for safely storing or preserving information for re-use within the LSRMS.

Representational State Transfer (REST): Is an architectural style that defines a set of constraints and properties based on HTTP.

Request for change (RFC): Is a document containing a call for an adjustment of a system; it is of great importance in the change management process.

Response Time (milliseconds - Network, Server): This metric tells is defined as the time it takes for any workload to place a request for work on the network, server or virtual environment and for the network, server or virtual environment to complete the request.

Responsible, Accountable, Consulted, Informed (RACI): Is an acronym that stands for responsible, accountable, consulted and informed. A **RACI** chart is a matrix of all the activities or decision making authorities undertaken in an organisation set against all the people or roles.

Root Cause Analysis: Describes a wide range of approaches, tools, and techniques used to uncover causes of problems.

S

Scalability: The ability of a system, network, or process to handle a varying workload in a capable manner or its ability to be enlarged to accommodate growth. This capability allows computer equipment and software programs to grow over time, rather than needing to be replaced. A scalable network should be able to support additional connections without data transfers slowing down. In each instance, scalable hardware can expand to meet increasing demands. While all hardware and software have some limitations, scalable equipment and programs offer a long-term advantage over those that are not designed to grow over time.

Schema: The structure that defines the organization of data in a database.

Scorecard: A strategy performance management tool - a semi-standard structured report, supported by design methods and automation tools that can be used to keep track of the execution of activities and to monitor the consequences arising from these actions.

Secure Access: The ability to permit or deny User access to resource(s) within the LSRMS.

Secure File Transfer Protocol (SFTP): The Secure File Transfer Protocol ensures that data is securely transferred using a private and safe data stream. It is the standard data transmission protocol for use with the SSH2 protocol.

Root Cause Analysis: Logical and physical boundary around network accessible resource(s) and information, which is controlled and protected against unauthorized access from outside of the boundary.

Security Assertion Markup Language (SAML 2.0): Is an umbrella standard that encompasses profiles, bindings and constructs to achieve Single Sign On (SSO), Federation and Identity Management. Security Assertion Markup Language is an XML-based open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider

Security Assessment and Authorization (SA&A):

Security Assessment: The on-going process of evaluating the performance of IT security controls throughout the lifecycle of information systems to establish the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the departmental business needs for security. Security assessment supports authorization by providing the grounds for confidence in information system security.

Security Authorization: The on-going process of obtaining and maintaining official management decision by a senior organizational official to authorize operation of an information system and to explicitly accept the risk of relying on the information system to support a set of business activities based on the implementation of an agreed-upon set of security controls, and the results of continuous security assessment.

Security Classification Level: An indicator of the sensitivity of the LSRMS information classifications specified by Government of Canada (GC)); (classification, abbreviation, sensitivity level)

a) Top Secret (TS) VH
b) Secret (S) H
c) Confidential (C) H
d) Protected 'C' (PC) H
e) Protected 'B' (PB) M
f) Protected 'A' (PA) L
g) Unclassified (U) VL
h) Non Sensitive (NS) VL

Security Control Profile (SCP): A security control profile is a set of IT security controls that an organization establishes as minimum mandatory requirements for their information systems.

Security High Level Design (SHLSD): The SHLSD is a more detailed version of the Security High-Level Service Design, that includes:

a) A detailed component diagram (this must be a refinement of the high-level component diagram);

b) Descriptions of the allocation of technical security mechanisms to detailed service design elements;

c) Descriptions of the allocation of non-technical security mechanisms to high-level organizational or operational elements; and

d) Justification for key design decisions

Security High Level Service Design (SHLSD): SHLSD includes:

a) A high-level component diagram that clearly shows the allocation of services and components to network security zones and identifies key security related data flows;
b) The architectural layers for example, communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer;
c) A description of the network zone perimeter defences;
d) A description of the use of virtualization technologies, where applicable;

e) Descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers;

f) Descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements; and

g) A description of the approach for:

i. Access Control
ii. Audit and Accountability
iii. Configuration Management
iv. Contingency Planning
v. Identification and Authentication
vi. Incident Response
vii. Media Protection
viii. Personnel Security
iv. Physical and Environmental Protection
v. Risk Assessment
vi. Security Awareness and Training
vii. System and Communications Protection
viii. System and Information Integrity
ix. System Maintenance
x. System and Services Acquisition

Security Integration test plan: An integration security test plan is the description of the steps required and the necessary tests to conduct in order to ensure that the security functions have been properly implemented at the integration phase of the solution (when the components of the solution are assembled to form the final solution).

Security Operations Center (SOC): The Security Operations Center is responsible for monitoring preventing, detecting, assessing and responding to cybersecurity threats and that can affect the system and the information within.

Security Requirements Traceability Matrix (SRTM): Is a grid that allows documentation and easy viewing of what is required for a system's security. SRTMs are necessary in technical projects that call for security to be included. Traceability matrixes in general can be used for any type of project, and allow requirements and tests to be easily traced back to one another. The matrix is a way to make sure that there is accountability for all processes and is an effective way for a User to ensure that all work is being completed.

Segmentation Rules eXchange (SRX): Is the vendor-neutral standard, originally published by LISA (Localization Industry Standards Association), for describing how translation and other language-processing tools segment text for processing.

Segments: Is a database that stores "**segments**" in a TM, which can be sentences, paragraphs or sentence-like units (headings, titles or elements in a list) that have previously been **translated**, in order to aid human translators.

Service Continuity Plan (SCP): Is a subset of Business Continuity Planning (BCP) and encompasses IT disaster recovery planning and wider IT resilience planning. It also incorporates those elements of IT infrastructure and services.

Service Level Agreement: Describes performance indicators or parameters, and the minimum values the provider commits to. The SLA often includes an up-time or availability percentage (99.9% or 99.99%) for some key functions, the performance of the service (or quality of service), the response time to incidents and issues, the time to fulfil certain service requests, and possibly other parameters of the service, such as the time to deploy patches, the time to replace parts, the time to notify incidents, etc.

Service Oriented Architecture (SOA): Is a style of software design where services are provided to the other components by application components, through a communication protocol over a network.

SIGMA (SAP –System Applications and Products): Manage PWGSC's financial, procurement and real property system in-service support – one of the most comprehensive SAP enterprise resource(s) planning systems within the Government of Canada.

Single Object Access Protocol (SOAP): Is a messaging protocol that allows programs that run on disparate operating systems (such as Windows and Linux) to communicate using Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML).

Single Sign On (SSO): Allows a single authentication credential--User ID and password, smart card, one-time password token or a biometric device--to access multiple or different systems within a single organization. A federated identity management system provides single access to multiple systems across different enterprises.

Snapshot: A view of data at a particular moment in time.

Software Release: Is a release that has usually gone through different steps in its development such as, alpha, beta, release candidate, general availability and production release.

Software Update: Are computer hardware and/or software patches of code that are released in order to address certain issues or to activate specific functionalities.

Software Upgrade: In computers, an upgrade is a newer version of or addition to a hardware or, software product that is already installed or in use.

Secure Sockets Layer (SSL): Was first versions of the protocol, Netscape (AOL).

Statement of Work (SOW): The part of a Contract which contains a comprehensive, narrative description of the work required. The SOW defines Tasks to be accomplished or services to be delivered in clear, concise and meaningful terms. It also stipulates the services or deliverables that are required to fulfill a Contract.

Storage: A function which involves the receipt of an item, putting it away for safekeeping and subsequent retrieval, when required for use, sale or disposal.

Structured Query Language (SQL): Is a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management.

Suppliers: A company that may have one or more resource(s) that can provide linguistics services to the Translation Bureau.

Support Request Delivery Channels (SRDC): Channels of communication that companies may offer to customers for support.

T

Task **Authorization (TA):** An administrative document that allows a User to authorize a Contractor to conduct work on an "as and when requested" basis in accordance with the terms and conditions of a Contract with Task Authorization.

TAUS Dynamic Quality Framework (TAUS DQF): Enables benchmarking, providing a framework of the best fit translation quality evaluation models based on content types.

Taxonomies: A way to classify and assign a structure to information.

Terabyte (TB): Is a measure of computer storage capacity that is a trillion bytes and more precisely defined as 1,024 gigabytes (GB).

TermBase eXchange (TBX): Is the international standard for representing and exchanging information about terminology

Threat and Risk Assessment (TRA): Structured process designed to identify risks and provide recommendations for risk mitigation through analysis of system / service critical assets, potential threat events / scenarios, and inherent vulnerabilities.

Throughput: Throughput refers to the performance of Tasks by a computing service or device over a specific period. For transaction processing systems, it is normally measured as transactions-per-second. For systems processing bulk data, such as audio or video servers, it is measured as a data rate (e.g., Megabytes per second). Web server throughput is often expressed as the number of supported Users – though clearly this depends on the level of User activity, which is difficult to measure consistently.

Traceability: The ability to verify the history, location, or application of an item by means of documented recorded identification.

Train the Trainer: A training program designed to teach participants how to deliver instructor-led, hands-on training for the service solution to Users.

Trainer: An individual who is responsible for teaching details relating to a service(s).

Transmission Control Protocol (TCP): Is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). The entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP.

Transport Layer Security (TLS): Is the new name for SSL. Namely, SSL protocol got to version 3.0; TLS 1.0 is "SSL 3.1". TLS versions currently defined include TLS 1.1 and 1.2. Each new version adds a few features and modifies some internal details. We sometimes say "SSL/TLS" (see *HTTPS*).

Translation Match Type Categories:

Repetitions - This row displays the number and/or percentage of words, characters or segments that are repetitions of previously counted words.

Context Match - This row displays the number and/or percentage of words, characters or segments for which a context match was found in the translation memory.

Exact Match - 100% the number and/or percentage of words, characters or segments for which a 100% translation memory match was found.

Fuzzy Match (95% - 99%), (85% - 94%), (75% - 84%), (50% - 74%) - These rows display the number and/or percentage of words, characters or segments that were translated with a less than perfect (100%) translation memory match. The degree of match is indicated by the percentage figure.

Internal Fuzzy Match (95% - 99%), (85% - 94%), (75% - 84%), (50% - 74%) - These rows display the additional leverage that can be obtained by the translator interactively translating the document with a translation memory. See Perform Internal Fuzzy Match Analysis for more details.

New - This row displays the number and/or percentage of words, characters or segments for which no match was found in the translation memory/memories.

Translation Memory (TM): Is a database that stores "segments", which can be sentences, paragraphs or sentence-like units that have previously been translated, in order to aid human translators that are saved so they can be applied to future translations.

Translation Memory Exchange (TMX 1.4B): File created in the Translation Memory Exchange (TMX) format, an open XML standard used for exchanging translation memory (TM) data created by Computer Aided Translation (CAT) and localization applications; may save words or phrases that have been translated from one language to another; used for transferring the translation memory between different tools and vendors.

Treasury Board Secretariat (TBS): Provides advice and makes recommendations to the Treasury Board committee of ministers on how the government spends money on programs and services, how it regulates and how it is managed.

U

Unauthorized Access: When an entity gains unauthorized access to a system in order to commit another crime such as destroying information contained in that system (e.g. infiltration, compromise, hacking, privilege escalation and unauthorized access/privilege).

Unicode Transformation Format (UTF): The Unicode Transformation Format (UTF) is a character encoding format which is able to encode all of the possible character code points in Unicode. The most prolific is UTF-8, which is a variable-length encoding and uses 8-bit code units, designed for backwards compatibility with ASCII encoding.

User: An individual authorized by the **Client** to use the **LSRMS** Solution under the Contract.

User Acceptance Testing (UAT): End User testing is a phase were the solution, system or application is tested to ensure it meets the requirements.

User Profile: Is a record of User-specific data that defines the User's working environment and role

V

Vertical Scaling: Vertical scaling can essentially resize your server with no change to your code. It is the ability to increase the capacity of existing hardware or software by adding resource(s) e.g. RAM, CPU, HD. Vertical scaling is limited by the fact that you can only get as big as the size of the server.

Virtualization: Is a software that separates physical infrastructures to create various dedicated resource(s) Virtualization software makes it possible to run multiple operating systems and multiple applications on the same server at the same time. The technology behind virtualization is known as a virtual machine monitor (VMM) or virtual manager, which separates compute environments from the actual physical infrastructure. This is done by installing a Hypervisor on top of the hardware layer, where The ***LSRMS Solution***s are then install. A hypervisor or virtual machine monitor (VMM) is computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine.

Virtual Private Network (VPN): Extends a private network across a public network, and enables Users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

W

Web Content Accessibility Guideline (WCAG): Defines how to make Web content more accessible to people with disabilities. Accessibility involves a wide range of disabilities, including visual, auditory, physical, speech, cognitive, language, learning, and neurological disabilities.

Web Services: A standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone. Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall.

What You See Is What You Get (WYSIWYG): Editor or program is one that allows a developer to **see** what the end result will look like while the interface or document is being created.

Word Perfect document (WPD): Is a text document file format.

Workflow Management: The routing of information to resource(s) along a prescribed process path associated with a particular service that can be automated and manually configured. The processes are configurable based on Tasks, business rules, policies and their specific steps (e.g. analysis, translation, review, validation, QA, editing and invoicing).

Workload Management: The ability to assign, schedule and manage Tasks and schedules of resource(s) , including the ability to assign workers to service lines, manage availability, level the volume and type of work Tasks across staff resource(s) as efficiently as possible, and in line with predetermined service-level objectives.

X

XML Localisation Interchange File Format (XLIFF): Is an XML-based format used to standardize the passing of data to and from tools during each step of the localization process. It standardizes the following:

Localized Content Processing
Translation Memory and Glossary Leveraging
CAT Tool, TMS, and MT Interaction
Localization Workflow Management

XLIFF is an XML-based format created to standardize the way localizable data are carried between individual steps of the localization process, while ensuring interoperability among the diverse tools in use. XLIFF files are bilingual documents containing the content that needs localization, its corresponding translations, as well as any auxiliary data that make the localization process efficient or even possible. Source language and target language data in XLIFF files are constantly in sync during the process.

As an open standard, XLIFF aims to eliminate a need for proprietary formats. It also allows interoperability, automation across workflows, and the ability to embed rules at the source. XLIFF standardizes aspects such as processing of localized content, leveraging TMs and glossaries, interaction with CAT tools, TMS or MT, as well as managing the overall localization workflow.

Y

Z

9 APPENDIX B – ACRONYMS

Acronym	Description
AA	Automated Attendant
AHES	After-hours emergency service
API	Application Programming Interface
ARA	Analytics, Reporting and Auditing
AU	Audit and Accountability
BIA	Business Impact Analysis
BI	Business Intelligence
CAB	Change Advisory Board
CASCO	Committee on Conformity Assessment
CAT	Computer Aided Translation
CAVP	Cryptographic Algorithm Validation Program
CEF	Common Event Format
CIOB	Chief Information Officer Branch
CISD	Canadian Industrial Security Directorate
CMS	Content Management System
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSV	Comma Separated Value
CWBS	Contract Work Breakdown Structure
DOC	Document, or an ASCII text file with text formatting codes in with the text; used by many word processors
DR	Disaster Recovery
DW	Data Warehouse
ETL	Extract Transfer and Load
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard**s**
FPOC	First Point of Contact
FTP	File Transfer Protocol
GC	Government of Canada
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTPS	HyperText Transfer Protocol Security
ID	Identification
IE	Internet Explorer
IEC	International Electro-technical Commission

Acronym	Description
IM	Instant Messaging
IM Architect	Information Management Architect
IP	Intellectual Property
IR	Incident Response
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LISA QA	Localization Industry Standards Association Quality Assurance
LSRMS	Linguistic Services Request Management System
MS Office	Microsoft Office
MT	Machine translation
NIST	National Institute of Standards and Technology
OCCI	Open Cloud Computing Interface
OCR	Optical Character Recognition
ODT	Open document text
OEM	Original Equipment Manufacturer
OLAP	Online Analytical Processing
OLTP	On-line Transaction Processing
OPC	Office of the Privacy Commissioner of Canada
OS	Operating System
PDF	Portable Document Format
PIPEDA	Personal Information Protection and Electronic Documents Act
PKI Entrust	Public Key Infrastructure Entrust
PMBOK	Project Management Body of Knowledge
PRINCE2	Projects IN Controlled Environments
PSPC	Public Services and Procurement Canada
QA	Quality Assurance
RACI	Responsible, Accountable, Consulted, Informed
REST	Representational State Transfer
RFP	Request for Proposal
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA&A	Security Assessment and Authorization
SAML 2.0	SAML 2.0 Security Assertion Markup Language

Acronym	Description
SAP	System Applications and Products
SCP	Security Control Profile
SCP	Service Continuity Plan
SDSD	Security Detailed Service Design
SHLSD	Security High Level Service Design
SLA	Service Level Agreement
SOA	Special Operating Agency
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SOW	Statement of Work
SRCL	Security Requirements Check List
SRDC	Support Request Delivery Channels
SRTM	Security Requirements Traceability Matrix
SRX	Segmentation Rules eXchange
SSC	Shared Services Canada
SSH	Secure Shell
SSL	Secure Socket Layer
SQL	Structured Query Language
SSO	Single Sign On
TA	Task Authorizations
TAUS DQF	TAUS Dynamic Quality Framework
TB	Translation Bureau
TBS	Treasury Board Secretariat
TBX	TermBase Exchange
TByte	Terabyte
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TM	Translation Memory
TMX	Translation Memory Exchange
UAT	User Acceptance Testing
UTF	Unicode Transformation Format
VPN	Virtual Private Network
WCAG	Web Content Accessibility Guidelines
WPD	Word perfect document
WS	Web Service
WYSIWYG	What You See Is What You Get
XLIFF	XML Localisation Interchange File Format
XLS	Microsoft Excel Spreadsheet
XLSX	Office Open XML Workbook (Spreadsheets)

Acronym	Description
XML	Extensible Markup Language

10 APPENDIX C – TRANSLATION BUREAU REPORTS

The following table is a list of report categories and types:

Report Category	Report Types
1.0 Production	a) Number of words, projects over a period, b) Distribution of projects by TB clients, applicants, specialties/domains, Task types, document types c) Distribution of internal vs. external Tasks, d) On-time delivery and past due, e) Urgent requests, f) After-hours emergency service (AHES), g) Deadline change requests, h) Summary by type of work and specialization.
2.0 Productivity	a) Timesheets by resource(s) , b) Productivity of resource(s) , c) Detail of Tasks performed by resource(s) , d) Details of Tasks and time spent per project, e) Details of Tasks and time spent per project by resource(s) , f) Overtime by directorate, division and resource(s) , g) Volume (hours and words) by specialty, by directorate, division and resource(s) , h) Number of tickets managed by resource(s) , i) Number of transactions by resource(s) ,
3.0 Financial	a) Revenues by TB client, domain, resource(s) , project, Task type b) Internal and external costs per TB client, c) Costs by internal and external resource(s) , d) Costs by cost centers, e) Costs by Task types, f) Detailed costs by TB clients, g) Receivables and payables.
4.0 Executive	a) Summary reports, b) Distribution of projects by TB clients and applicants, c) Cost and benefit analysis, d) On-time delivery and past due, e) Urgent requests, f) After-hours emergency service (AHES), g) Deadline change requests, h) Costs by cost centers, i) Detailed costs by TB clients, j) Receivables and payables.
5.0 Tools	a) Number of words and cost savings per type of memory used, b) Overall redundancy statistics per period, c) Percentage of CAT translated segments left as is in the final translations.
6.0 Interpretation	Volume Conference and Parliament Interpretation Service; a) Interpreter-Days,

Report Category	Report Types
	b) Converted hours, c) Workload distribution internal / external Conference, Parliament, and Visual Interpretation Service; d) Hours of work per day, week, month, TB client, interpreter, region, and language. e) Hours of paid travel time per day, week, month, TB client, interpreter, region, and language. f) Number of contracts (open and punctual) per day, week, month, TB client, interpreter, region, and language. g) Number of events per day, week, month, TB client, interpreter, region, and language. Service Standards Conference, Parliament, and Visual Interpretation Service; a) Number of events refused, b) Time required to process an interpretation request, c) Time required to invoice a request, d) Time required to assign interpreters to an event, Other Conference and Parliament Interpretation Service; a) Number of Contractor s and rates (average rate, highest rate, lowest rate) per day, hour. b) Security clearance: Report on interpreter, c) Broadcasting Premiums, d) Number of events modified after confirmation by TB client (signed contract), e) Number of events reactivated after cancellation, f) Multilingual Premiums, g) Help offered / Help received, h) Remote / Hybrid Assignments. i) Number of events by priority (Conference Interpretation)

11 APPENDIX D – PROFESSIONAL SERVICES RESOURCE(S) RESPONSIBILITIES

Project Manager

Responsibilities could include but are not limited to:

- Perform overall project planning based on predefined Charters, estimates, schedules and scope;
- Manage, monitor and forecast project execution;
- Take corrective action as required to deliver project within scope, quality, time and budget (including scope change management and risk mitigation);
- Ensure internal and external stakeholders management through effective communication;
- Manage end-to-end tactical projects of various sizes;
- Maintain existing plans, PMO tools, procedures and systems in use within the PMO that are needed to manage and direct PMO development activities;
- Develop and produce new plans and procedures (in writing and subject to acceptance by the Project Authority(s)) required by the directorate to manage and direct the PMO development activities;
- Plan, organize and coordinate all activities related to an assigned project including all financial, planning and scheduling aspects;
- Define and document the objectives for the project and determine the budgetary requirement;
- Produce and maintain integrated work breakdown structures (WBS) and schedules;
- Analyze integrated schedules to identify priorities, activities and conflicts and advise solutions to senior and other project managers;
- Communicate plans, progress and developments to client management;
- Manage the implementation of the following management processes at the Directorate level with regards to Issues, Risk, Quality, Performance and Change;
- Manage project teams as defined in the project charter (including Tasks assignments and performance reviews);
- Plan and coordinate the activities of project personnel and other support providers;
- Manage the team members within project boundaries;
- Negotiate scope, resource(s) and schedule changes with stakeholders;
- Contribute to projects life-cycle improvements through lessons learned and project archives;
- Report to a mid-level organizational manager that has authority over most of the people on the project team; and
- Manage projects that may be under the guidance of a more senior project manager, subordinate to other project coordinators and leaders as well as other project managers at the Senior and Executive levels.

System Analyst

Responsibilities could include but are not limited to:

- Develop requirements, feasibility, cost, design, and specification documents for systems.
- Implement systems to support projects, departments, organizations or businesses.
- Translate business requirements into systems design and specifications.
- Analyze and recommend alternatives and options for solutions.
- Develop technical specifications for systems development, design and implementation.

Data Conversion Specialist

Responsibilities could include but are not limited to:

- Oversee all facilities of the conversion process.
- Complete mapping, interfaces, mock conversion work, enhancements, actual conversion, and verify completeness and accuracy of converted data.
- Establish a strong working relationship with all clients, interact effectively with all levels of client personnel, and provide conversion support.
- Analyze and coordinate data file conversions.
- Work with importing files from heterogeneous platforms.

Business Analyst

Responsibilities could include but are not limited to:

- Develop and document statements for considered alternatives.
- Perform business analyses of functional requirements to identify information, procedure, and decision flows.
- Evaluate existing procedures and methods, identify and document items such as database content, structure, application subsystems.
- Define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems.
- Establish acceptance test criteria with **Client**.
- Support and use the selected departmental methodologies.

Business Process Re-engineering (BPR) Consultant

Responsibilities could include but are not limited to:

- Review existing work processes and organizational structure.
- Analyze business functional requirements to identify information, procedures and decision flows.
- Identify candidate processes for re-design; prototype potential solutions, provide trade-off information and suggest a recommended course of action. Identify the modifications to the automated processes.
- Provide expert advice in defining new requirements and opportunities for applying efficient and effective solutions; identify and provide preliminary costs of potential options.
- Provide expert advice in developing and integrating process and information models between processes to eliminate information and process redundancies.
- Identify and recommend new processes and organizational structures.
- Provide expert advice on and/or assist in implementing new processes and organizational changes.
- Document workflows.
- Use business, workflow and organizational modeling software tools.

12 APPENDIX E – INTERPRETATION WORKLOAD CALCULATION AND EXAMPLE

The following is an excerpt from the Translation Collective Agreement that outlines the information used to calculate the total number of hours worked by Conference and Parliament interpreter employees.

12.1 Hours of work - Interpreters

a) On average, an interpreter's normal work day shall consist of six (6) hours of interpretation when part of a team of three (3) interpreters for a meeting in a single bilingual booth, (or a team of two (2) interpreters for a meeting in a trilingual booth), or approximately four (4) hours of interpretation when part of a team of two (2) interpreters for a meeting in a single bilingual booth.

b) The number and make-up of the teams of interpreters shall be determined on the basis of the workload.

I. For simultaneous interpretation, the minimum number is:
In the case of meetings involving two (2) working languages, three (3) interpreters in a single bilingual booth working for up to six (6) hours (it being understood that a team should not normally work for more than four (4) consecutive hours); or

Two (2) interpreters working for up to four (4) hours (it being understood that a team should not normally work for more than three (3) consecutive hours). In the case of meetings involving three (3) working languages, at least two (2) interpreters per unilingual booth working for up to six (6) hours (it being understood that a team should not normally work for more than four (4) consecutive hours).

In the case of meetings involving four (4) working languages, at least two (2) interpreters per unilingual booth working for up to six (6) hours, and three (3) interpreters where conditions warrant (it being understood that a team should not normally work for more than four (4) consecutive hours).

At the House of Commons, teams shall consist of three (3) interpreters per booth and should not normally work for more than six (6) consecutive hours. The Employer, after consultation with the Association, shall establish the roster of interpreters accordingly.

II. For consecutive, elbow or escort interpretation, the number of interpreters on the team shall normally be at least two (2) interpreters working a six (6)-hour day.

c) The total hours of work may vary depending on operational requirements. However, the hours of work shall be balanced on a monthly basis or, when possible, twice a month, with the Employer making every reasonable effort not to assign more than thirty-seven decimal five (37.5) hours of work per week, as a general rule. Work shall be calculated in hours, with one hour of interpretation equaling one point two five (1.25) hours of work in the case of a team of three (3) interpreters and one point eight seven five (1.875) hours of work in the case of a team of two (2) interpreters in a meeting involving two working languages working in a single bilingual booth.

For elbow, consecutive or escort interpretation, one (1) hour of interpretation shall equal one point eight seven five (1.875) hours of work when the interpreter is alone and one point two five (1.25) hours of work when the interpreter is part of a team.

The calculation of hours of work shall include all duties expressly authorized by the Employer, as well as leaves and holidays.

d) As a general rule, interpretation assignments shall be scheduled within time blocks that begin at the time the interpreter is required to report for duty and end twelve (12) hours later. The interpretation time of each assignment is counted in minutes, beginning at the time recorded on the interpreter's program and ending at the time the interpreter's presence is no longer required.

e) Where operational requirements allow it, the Employer, when scheduling the interpreter's program, shall normally allow for a twelve (12)-hour interval between the end of the interpreter's work day and the start of his or her next time block.

f) Where operational requirements allow it, the Employer shall grant the interpreter two (2) consecutive days of rest during each seven (7) calendar day period. Should it not be possible to grant such a rest period, these days of rest shall be reinstated as soon as possible through the operation of the monthly balancing process set out in paragraph (c) above.

g) Pursuant to paragraph (c), the Employer shall post the interpreters' weekly and cumulative hours worked. Moreover, where the Conference Interpretation Service is concerned, the Employer shall post fortnightly the assignment program for the next two (2) weeks.

h) An interpreter whose interpretation assignment is cancelled and who is not reassigned for an equivalent period during the same time block shall be deemed to have performed duties other than interpretation during the idle portion of the scheduled assignment.

i) An interpreter who is required by the Employer to be on standby for a specified period shall remain available for the duration of that period at a known telephone number and shall stand ready to report for duty as quickly as possible if called. This period shall be deemed part of the time block for the purposes of paragraph (d).

Note: The coefficients allow hours to be converted in order to determine the work volume per day / week / month. The rest days are also awarded based on number of hours per week or per month. Coefficients are used, daily to calculate and distribute workload, and once or twice a month to balance the hours for example, rest days.

12.2 EXAMPLE CALCULATION - HOURS OF WORK - INTERPRETERS

Day	Activity	Calculation	Total (Hrs)
Monday	4 hrs of interpretation (team of two, bilingual booth)	4 * 1.875	7.5
Tuesday	Day of rest		7.5
Wednesday	8 hrs of interpretation (team of 3, bilingual booth	8 * 1.25	10
Thursday	Translation for 4 hrs. 2hrs of interpretation (team of 3, bilingual booth)	4 + (2*1.25)	6.5
Friday	8 hrs of interpretation (team of 3, bilingual booth	8 * 1.25	10
Saturday	Did not work		
Sunday	2 hrs of interpretation (team of two, bilingual booth)	2 * 1.875	3.75
Total for the week			45.25 hrs

13 APPENDIX F - TRANSLATION BUREAU LANGUAGES AND FILE FORMATS

13.1 LANGUAGES

Translation Bureau Languages
English
French
Unknown
Afrikaans
Albanian
Algonquin
German
Amharic
Ancient Greek
Arabic
Armenian
Assamese
Assyrian
Atikamekw
Awadhi
Azerbaijani
Azeri
Bambara
Basque
Bengali
Belarusian
Bihari
Burmese
Bislama
Blackfoot
Blin
Boharme
Bosnian
Brazilian
Bulgarian
Buryat
Cambodian
Cantonese - Chinese Yuy (interpretation)
Carrier
Catalan
Cebuano
Chilcotin
Chinese
Chinese (simplified)
Chinese (traditional)
Korean
Woodland Cree
Creole
Kazakh
Kinyarwanda
Kyrgyz
Kirundi
Kurdish
Kwak'wala
Laotian
Latin
Latvian
Lil'wat
Lingala
Lithuanian
Luganda
Luhya
Macedonian
Malay
Malayalam
Maliseet
Malagasy
Maltese
Mandarin - Chinese (Interpretation)
Mandingo
Marathi
Michif
Mi'kmaq
Smith-Francis Mi'kmaq
Pacific Mi'kmaq
Mina
Mohawk
Mongolian
Montagnais
Moose Cree
Mowachaht
Naskapi
Dutch
Nepalese
Nisga'a
Northern Tutchone
Norwegian
Nunavik
Nuu Chah Nulth
Oji-Cree
Ojibwe

Translation Bureau Languages

Cree
Cree - Swampy
Central/Swampy Cree
Northern Cree of Quebec
Swampy Cree - Ontario
Swampy Cree - Saskatchewan
Swampy Cree - Manitoba - Syllabic Characters
Swampy Cree - Manitoba - Roman Characters
Croatian
Dakota
Danish
Dari
Denesuline
Ditidaht
Dogrib
Duri
Edo
North Slavey
South Slavey
Spanish
Esperanto
Estonian
Ewe
Fanti
Faroese
Finnish
Flemish
Fulfulde
Scottish Gaelic
Welsh
Georgian
Gujarati
Greek
Gwich'in
Halq'eméylem
Hebrew
Rabbinic Hebrew
Hindi
Hungarian
Hul'q'umi'num
Igbo
Ilocano
Ilongo
Indonesian
Innu- aimun
Inuinnaqtun
Inuktitut

Oowekyala
Oromo
Udi
Wolof
Urdu
Uzbec
Pashto
Punjabi
Punjabi (Arabic script)
Persian
Filipino
Plains Cree
Polish
Portuguese
Pular
Quebec Cree
Rainy River Ojibwe
Romanian
Russian
Coast Salish
Sanskrit
Saulteaux
Secwepemctsin
Serbian
Serbo-Croatian
Setswana
Shona
Sindhi
Sinhalese
Slovakian
Slovenian
Somalian
Susu
Stoney
Swedish
Swahili
Tajik
Tagalog
Tamil
Tatar
Tchech
Chechen
Chee
Telugu
Thai
Tibetan
Tigrinya

Translation Bureau Languages	
Labrador Inuktitut Inuvialuktun Irish Icelandic Italian Japanese Javanese Kannada S'gaw Karen Kaska	Toro Tshiluba Turkish Uyghur Ukranian Vietnamese Old Portuguese Yiddish Yoruba Zulu

13.2 FILE FORMATS

File Formats (extension)	File Format Description
xls, xlsx, xlsb	Excel document
xltx, xltm, xlt	Excel template
csv, prn, dif, slk	File of values, can be opened by Excel
xla, xlam	Excel macro file
ods	OpenOffice equivalent of Excel
doc, docx, docm	Word document
dot, dotx, dotm	Word template
odt	OpenOffice equivalent of Word
wpd	WordPerfect document
lwp	WordPro document
ppt, pptx, pptm	PowerPoint document
potx, potm, pot	PowerPoint template
ppsx, ppsm, pps	PowerPoint slide show
ppam, ppa	PowerPoint add-in
odp	OpenOffice equivalent of PowerPoint
VSD, VSS, VST, VSW, VDX, VSX, VTX, VSDX, VSDM, VSSX, VSSM, VSTX, VSTM, VSL	Visio document
pub	Publisher document
txt	Text document
mht, mhtml, htm, html	Web page

File Formats (extension)	File Format Description
rtf	Written document
pdf	Portable document file
xps	Similar to a PDF
msg	Outlook email
oft	Outlook template
wps	Works document
one	OneNote file
accdb, accdt, mdb	Access database
xml	Text file that can be opened by just about anything
mp4, wmv, MPG, MP2, MPEG,	Video file
mp3, dss	Audio file
gif, jpg, png, tif, bmp, wmf, emf, svg, webp	Image file
zip	Compressed file
tmx	Translation memory file
tbx	Terminology data file (glossary)

14 APPENDIX G – SECURITY AND PRIVACY

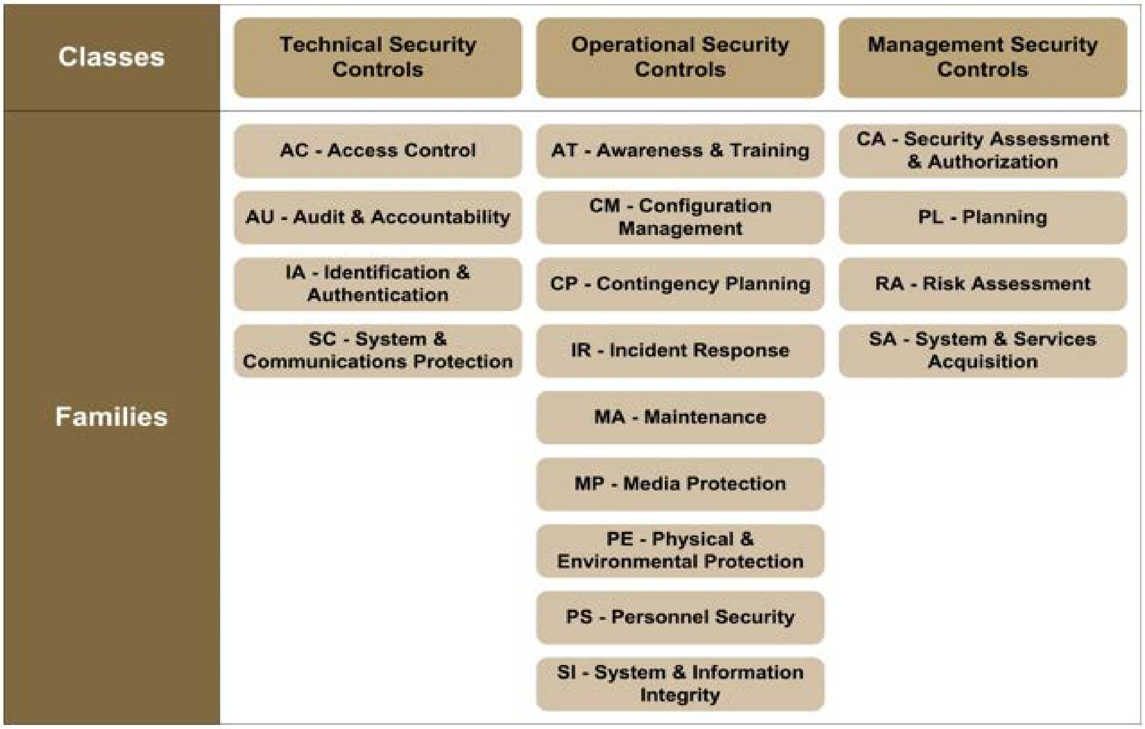
14.1 ITSG-33 CONTROL FAMILIES

The SCP is comprised of security controls defined by Communications Security Establishment (CSE).

The controls are catalogued in the CSE guidance document: ITSG-33, IT security risk management: a lifecycle approach.

Security controls within ITSG-33 are divided into 3 classes: technical, operational and management.

Within those 3 classes the controls are further subdivided into the following seventeen (17) families:



Classes	Technical Security Controls	Operational Security Controls	Management Security Controls
Families	AC - Access Control	AT - Awareness & Training	CA - Security Assessment & Authorization
	AU - Audit & Accountability	CM - Configuration Management	PL - Planning
	IA - Identification & Authentication	CP - Contingency Planning	RA - Risk Assessment
	SC - System & Communications Protection	IR - Incident Response	SA - System & Services Acquisition
		MA - Maintenance	
		MP - Media Protection	
		PE - Physical & Environmental Protection	
		PS - Personnel Security	
		SI - System & Information Integrity	

14.1.1 LSRMS ITSG-33 Security Controls

The LSRMS Security Controls are based on the ITSG-33 controls and are presented below. The controls have a cross-reference to the identifiers used in ITSG-33.

The following table lists the ITSG-33 Security Controls families that are included:

Control Families	Description	Acronym
Access Control	Security controls that support the ability to permit or deny User access to resource(s) within the information system	AC
Audit and Accountability	Security controls that support the ability to collect, analyze, and store audit records associated with User operations performed within the information system.	AU
Configuration Management	Security controls that support the management and control of all components of the information system (e.g., hardware, software, and configuration items).	CM

Control Families	Description	Acronym
Contingency Planning	Security controls that support the availability of the information system services in the event of component failure or disaster.	CP
Identification and Authentication	Security controls that support the unique identification of Users and the authentication of these Users when attempting to access information system resource(s) .	IA
Incident Response	Security controls that support the detection, response, and reporting of security incidents within the information system.	IR
Media Protection	Security controls that support the protection of information system media (e.g., disks and tapes) throughout their life cycle.	MP
Personnel Security	Security controls that support the procedures required to ensure that all personnel who have access to the information system have the required authorizations as well as the appropriate security screening levels.	PS
Physical and Environmental Protection	Security controls that support the control of physical access to an information system as well as the protection of the environmental ancillary equipment (i.e., power, air conditioning and wiring) used to support the operation of the information system.	PE
Risk Assessment	Security controls that deal with the conduct of risk assessments and vulnerability scanning.	RA
Security Awareness and Training	Security controls that deal with the education of Users with respect to the security of the information system.	AT
System and Communications Protection	Security controls that support the protection of the information system itself as well as communications with and within the information system.	SC
System and Information Integrity	Security controls that support the protection of the integrity of the information system components and the data that it processes.	SI
System Maintenance	Security controls that support the maintenance of the information system to ensure its ongoing availability.	MA
System and Services Acquisition	Security controls that deal with the contracting of products and services required to support the implementation and operation of the information system.	SA

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-1	Access Control	The Contractor should: a) Develop, disseminate, and review/update annually, the access control policies and associated access control requirements for ***LSRMS Solution*** Infrastructure components; and b) Provide TB with the operational security procedures that include operational roles and responsibilities for access control EVIDENCES: a) Name of Policy Instrument: *LSRMS Security Policy,* Section 4 Access Control, pages 55-63 Access Control Sub-Sections 4.1 Scope, 4.2 Policy Update and Renewal Schedule, 4.3 Roles and Responsibilities, 4.4 AC Governance, 4.5 Inter-Organization Coordination, 4.6 AC implementation, 4.7 Account Management, b) Access Control Sub-Sections 4.1 Scope, 4.2 Policy Update and Renewal Schedule, 4.3 Roles and Responsibilities, 4.4 AC Governance, 4.5 Inter-Organization Coordination, 4.6 AC implementation, 4.7 Account Management,	AC-1
SR-2	Access Control	The Identity Credential and Access Management Service should automatically provision Accounts for LSRMS User Accounts and Generic Accounts, as follows: a) Assign a unique LSRMS Account and Display Name in accordance with the standard to be defined in the tailoring process, by applying configurable naming and conflict resolution rules; b) Create an Account with no privileges; c) Assign a one-time temporary password to the Account; d) Assign Account attributes and security access privileges as specified by TB; and e) Return the assigned LSRMS Account, Display Name, and one-time password to the Account Requester. (A) LSRMS should support different types of user accounts, including the following:	AC-2

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		Contractor administrative (and other contractor account types as required) a) Client accounts b) TB user accounts c) TB user management accounts d) (and other types of accounts to be defined in the security controls tailoring phase). (B) The user management accounts should be able to create, activate, deactivate and delete user accounts. (C) The Contractor will implement functionality to enable the establishment of group and role membership, and allow TB user management accounts to assign membership. (G) The Contractor provides functionality to monitor the use of user accounts and that functionality is accessible to the user management accounts. (L) LSRMS will generate one-time temporary password at account creation (that will be sent to the user via secure email to be defined at the tailoring phase).	
SR-3	Access Control	The system should: a) Prevent the re-use of a LSRMS Account as specified by TB; b) Allow Account suspension policies as specified by TB; c) Not allow access to a suspended Account; d) Not allow an Account to send and receive LSRMS work flow messages if the Account is suspended; and e) Not allow direct access to the LSRMS Solution Service Infrastructure for any Account, as specified by TB.	AC-2
SR-4	Access Control	The Contractor should manage LSRMS Infrastructure Operators accounts by: a) Identifying account types (i.e., individual, group, system, device, application, guest/anonymous, and temporary); b) Establishing conditions for group membership; c) Identifying authorized Operators of the LSRMS Infrastructure and specifying access privileges; d) Requiring appropriate approvals for requests to establish accounts; e) Selecting an identifier that uniquely identifies the Operator or device;	AC-2(2)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		f) Assigning the Operator identifier to the intended party or the device identifier to the intended device; g) Establishing, activating, modifying, disabling, and removing accounts; h) Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; i) Notifying account administrator when temporary accounts are no longer required and when LSRMS Infrastructure Operators are terminated, transferred, or LSRMS Infrastructure usage or need-to-know/need-to-share changes; j) Preventing reuse of identifiers for at least one year; k) Deactivating: i. Temporary accounts that are no longer required; ii. Accounts of terminated or transferred Operators; iii. Accounts after a number of day of inactivity as specified by TB, and iv. Temporary and emergency accounts over a given age; l) granting access to the LSRMS Infrastructure based on: i. a valid access authorization; ii. intended system usage, and iii. other attributes as required by the Contractor or TB; m) Reviewing accounts at least monthly; n) Locking the account after ten (10) unsuccessful login attempts occurring within five (5) minutes, and o) Keeping the account locked until manually unlocked by another Operator.	
SR-5	Access Control	The LSRMS should log the following events: a) Account creation; b) Account modifications c) Account suspension; d) Account termination; e) Account deletion; and f) Account views of LSRMS accounts of which the User is not the primary owner.	AC-2(4)
SR-6	Access Control	The LSRMS Infrastructure should enforce access authorizations for Operators.	AC-3
SR-7	Access Control	The LSRMS information system does not release information outside of the established system boundary unless PSPC	AC-3 (9)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		security safeguards and procedures are used to validate the appropriateness of the information designated for release.	
SR-8	Access Control	The Contractor should implement separation of duties for Operators, as necessary, to prevent malevolent activity without collusion according to the role-based access profile assigned to the Operator. The Contractor should document the separation of duties.	AC-5
SR-9	Access Control	The Contractor should implement a least privileges policy for LSRMS Infrastructure Operators as follows: a) the access control mechanisms should be configured to implement least privilege, allowing only authorized accesses for Operators (and processes acting on their behalf) that are necessary to accomplish assigned tasks; b) create non-privileged accounts to be used for non-operations tasks; c) restrict authorization to super user accounts (e.g., root) to designated Operators; d) prevent sharing of Operator accounts; and e) should uniquely identify the human Operator who has performed each operation on the LSRMS Infrastructure.	AC-6
SR-10	Access Control	The LSRMS must: a) display a logon banner (defined during the tailoring phase) approved by TB on the login page of any web-based application for Users. b) include an access control mechanism that: i. Prevents access to LSRMS Infrastructure components or resources without identification, authentication, and authorization; ii. Displays a TB-approved logon warning banner that authorized operators must acknowledge prior to being granted access to LSRMS Infrastructure components; iii. Notifies the operators, upon successful logon (access), of the date and time of the last logon (access), and iv. Uses a readily observable logout capability whenever authentication is used to gain access to LSRMS Infrastructure components. c) include an operator session lock mechanism that:	AC-8

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		i. Prevents further access to Infrastructure components by automatically initiating an operator session lock after a period of inactivity no longer than 60 minutes; ii. Prevents further access to Infrastructure components by initiating an operator session lock when requested by the operators; iii. Displays a screen saver that contains no meaningful information to completely replace what was previously displayed on the screen upon activation of an operator session lock, and iv. Unlocks an operator session after successful authentication of the operator. d) include an access control mechanism that: i. Prevents User access to LSRMS functionality, components or resources without identification, authentication, and authorization; ii. Displays TB-approved system use information that authorized users must acknowledge prior to being granted access to LSRMS; iii. Notifies the Users, upon successful logon (access), of the date and time of the last logon (access), and iv. Uses a readily observable logout capability whenever authentication is used to gain access to LSRMS. e) Displays a description of the authorized uses of the system f) Displays the maximum classification level that the system can store and process ("Protected B")	
SR-11	Access Control	The Contractor should ensure that any use of Remote Management within the LSRMS Infrastructure take place using a method approved by TB that includes: a) Remote Management should be restricted to LSRMS Infrastructure located within a contractor Service Delivery Point using LSRMS dedicated management consoles; b) Documenting allowed methods of Remote Management and establish usage restrictions and implementation guidance for each allowed remote management method; c) monitoring for unauthorized Remote Management;	AC-17

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		d) authorizing Remote Management prior to connection; e) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods; f) routing all Remote Management to LSRMS Infrastructure components through a limited number of managed access control points; g) protecting information about Remote Management mechanisms from unauthorized use and disclosure; and h) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods. The Contractor should provide secure mechanisms for remote access (outside of GC networks) for users that do not have secure mechanisms to remotely access GC networks prior to accessing LSRMS.	
SR-12	Access Control	The Contractor must establish Policies and procedures, supporting business processes and implement technical measures to protect LSRMS from wireless network environments, including the following: a) Perimeter firewalls implemented and configured to restrict unauthorized traffic b) Security settings enabled with strong encryption for authentication and transmission in compliance with CSEC`s ITSP.40.111 for "Protected B" data c) Security hardening by replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) d) User access including Operators to wireless network devices restricted to authorized personnel e) The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network.	AC-18
SR-13	Access Control	The Contractor should implement a mobile device policy for LSRMS that includes the following at minimum a) Anti-malware awareness training, specific to mobile devices, should be included in the Contractor's information security awareness training; b) A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data;	AC-19

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		c) The contractor should have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store. d) If Applicable, the Bring Your Own Device (BYOD) policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage. e) The contractor should have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The Contractor should post and communicate the policy and requirements through the company's security awareness and training program. f) All cloud-based services used by the company's mobile devices or BYOD should be pre-approved for usage and the storage of LSRMS business data. g) The contractor should have a documented application validation process to test for mobile device, operating system, and application compatibility issues. h) The BYOD policy should define the device and eligibility requirements to allow for BYOD usage. i) Contractor should keep and maintain an inventory of all mobile devices used to store and access LSRMS data. j) Contractor should include for each device in the inventory details of all changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)). k) A centralized, mobile device management solution should be deployed to all mobile devices permitted to store, transmit, or process LSRMS data. l) The mobile device policy should require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices, and should be enforced through technology controls. m) The mobile device policy should prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and should enforce the prohibition through detective and	

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		preventative controls on the device or through a centralized device management system (e.g., mobile device management). n) The BYOD policy, if applicable, should include clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy should clearly state the expectations regarding the loss of non LSRMS business data in the case a wipe of the device is required. o) BYOD and/or contractor-owned devices are configured to require an automatic lockout screen, and the requirement should be enforced through technical controls. p) Changes to mobile device operating systems, patch levels, and/or applications should be managed through the Contractor's change management processes. q) Password policies, applicable to mobile devices, should be documented and enforced through technical controls on all contractor devices or devices approved for BYOD usage, and should prohibit the changing of password/PIN lengths and authentication requirements. r) The mobile device policy should require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported). s) All mobile devices permitted for use through the Contractor’s BYOD program or a company-assigned mobile device should allow for remote wipe by the Contractor's corporate IT or should have all company-provided data wiped by the Contractor's corporate IT. t) Mobile devices connecting to contractor networks, or storing and accessing company information, should allow for remote software version/patch validation. u) All mobile devices should have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel should be able to perform these updates remotely.	

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		v) The BYOD policy should clarify the systems and servers allowed for use or access on a BYOD-enabled device.	
SR-14	Access Control	The Contractor should obtain TB's approval for the use (access, process, store, or transmit information) of external (i.e., non-Contractor) information systems for the delivery of LSRMS.	AC-20
SR-15	Access Control	The Contractor should limit the use of Contractor-controlled portable storage media within the LSRMS (e.g., thumb drive) as follows: a) Restrict the use to authorized Operators only, and b) Restrict the use to LSRMS Infrastructure components only. The selection and use of portable data storage devices should be in accordance with TBS's ITPIN: 2014-01.	AC-20(2)
SR-16	Security Awareness and Training	The Contractor should provide TB with the LSRMS operational security policies and procedures that include operational roles and responsibilities for awareness and training. The Contractor should review and update the security awareness and training policy (at least every 3 years) and procedures (at least every year) and provide them to TB.	AT-1
SR-17	Security Awareness and Training	The Contractor should provide security awareness and training for LSRMS Infrastructure Operators as follows: a) As part of initial training for new Operators; b) Before authorizing access to the LSRMS Infrastructure or performing assigned duties, and c) Annually or when security impacting changes to the LSRMS occur.	AT-2, AT-3
SR-18	Security Awareness and Training	The Contractor should monitor and document LSRMS security awareness and training for LSRMS Infrastructure Operators including: a) Documenting who received what training course and when, and b) Retaining records for the last three (3) years.	AT-4
SR-19	Audit and Accountability	The Contractor should provide TB with the LSRMS operational security procedures that include operational roles and responsibilities for audit and accountability. The Contractor reviews and updates the procedures that include operational roles and responsibilities for audit and accountability at least every year.	AU-1

Security Requirement IDs (for Canada's purpose only)	**Requirement Category**	**Description**	**ITSG-33**
SR-20	Audit and Accountability	The LSRMS Identity Credential and Access Management Service should log the following events in accordance with the authentication event logging requirements for LoA3, as detailed in ITSP.30.031 V3 (https://www.cse-cst.gc.ca/en/node/1842/html/26717). a) Successful authentication events; and b) Unsuccessful authentication events.	AU-2
SR-21	Audit and Accountability	The Contractor should a) Review and update the list of auditable events for LSRMS at minimum once in 180 business days ; b) Include execution of privileged functions in the list of auditable events; c) Log events as identified and approved by TB; and d) Automatically generate real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise.	AU-2(3)
SR-22	Audit and Accountability	The Contractor should ensure that the LSRMS: a) Produces audit records that contain sufficient information, as defined by TB, to, at a minimum, establish: i. What type of event occurred, ii. When (date and time) the event occurred, iii. Where the event occurred, the source of the event, iv. The outcome (success or failure) of the event, and v. The identity of any user/subject associated with the event; b) Produces audit events identified by type, location, or subject; and c) Manages the content of audit records that are generated.	AU-3
SR-23	Audit and Accountability	The Contractor should perform capacity management on the LSRMS audit record storage by: a) Allocating enough audit record storage capacity (to be defined during the tailoring process); b) Configuring auditing to prevent storage capacity being exceeded; c) Alerting the Operations Center when the allocated audit record storage volume reaches 75% of the audit record storage capacity; and d) Overwriting the oldest audit records if storage reached maximum capacity.	AU-4, AU-5(1)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-24	Audit and Accountability	The LSRMS audit function should respond to auditing failures by: a) alerting the Operations Center and TB (for audit events to be defined during the tailoring process); and b) Overwriting the oldest audit records if storage reached maximum capacity.	AU-5
SR-25	Audit and Accountability	The LSRMS should use internal system clocks that are synchronized with an authoritative time source, approved by TB, to generate time stamps for audit records.	AU-8, AU-8(1)
SR-26	Audit and Accountability	The LSRMS should: a) Protect audit information from unauthorized access, modification, and deletion; and b) Backup audit records onto a different system or media than the system being audited on a schedule as specified by TB.	AU-9, AU-9(1), AU-9(2), AU-9(3), AU-9(4)
SR-27	Security Assessment and Authorization	The Contractor should conduct vulnerability assessments a) Before LSRMS goes into production b) At least once per year; and c) When there are significant changes that may impact the security of the system The Contractor should develop a LSRMS vulnerability mitigation plan approved by TB within five (5) business days of completion of a vulnerability assessment that includes proposed protection measures to mitigate the risks identified from the vulnerability assessment.	CA-7(2)
SR-28	Configuration Management	The Contractor should develop, document, and maintain under configuration control, a current baseline configuration of the LSRMS Infrastructure components and the two (2) previous versions.	CM-2, CM-2(1), CM-2(2), CM-2(3), CM-2(4)
SR-29	Configuration Management	The Contractor should only allow authorized software, as documented by the Contractor and approved by TB, to execute on the LSRMS.	CM-2(5)
SR-30	Configuration Management	The Contractor should: a) Plan and test the implementation of new and changed software, hardware and documentation for a LSRMS release not using the production environment or the control test environment of the LSRMS; b) Implement new and changed software, hardware and documentation for a LSRMS release as approved by TB; and	CM-3(2), CM-3(3), CM-3(4)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		c) Develop and implement procedures for the distribution, installation, and rollback of changes implemented for a LSRMS release.	
SR-31	Configuration Management	The Contractor should assess the security impact of changes by: a) Analyzing new software before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice; b) Informing TB of potential security impacts prior to change implementation, and c) Checking the security functions, after changes are implemented, to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the applicable security requirements.	CM-4
SR-32	Configuration Management	The Contractor should conduct audits of information system changes at least every 12 months and when indications so warrant, determining whether unauthorized changes have occurred.	CM-4
SR-33	Configuration Management	The Contractor should review LSRMS Infrastructure Operator privileges on a quarterly basis.	CM-5(5)
SR-34	Configuration Management	The Contractor should employ automated mechanisms to centrally manage, apply, and verify configuration settings for all components of the LSRMS, including products from other vendors included in the solution. Any deviation from the established configuration settings should be identified and documented. The Contractor should monitor and control changes to configuration settings.	CM-6, CM-6(1), CM-6(2)
SR-35	Configuration Management	The Contractor should open a Security Incident Ticket when an unauthorized configuration change is detected in the LSRMS.	CM-6(3)
SR-36	Configuration Management	a) The Contractor should configure the LSRMS to provide only essential capabilities, all non-essential capabilities should be disabled. b) The Contractor prohibits or restricts the use of the following functions, ports, protocols, and/or services: to be defined during the tailoring process and approved by TB. c) The Contractor reviews the information system monthly to identify unnecessary and/or non-secure functions, ports, protocols, and services; and	CM-7, CM-7(1), CM-7(2), CM-7(3), CM-7(5)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		d) The Contractor disables functions, ports, protocols, and services within LSRMS deemed to be unnecessary and/or non-secure. e) The Contractor uses a registration process (and ensures compliance to it) to manage, track, and provide oversight for the system and its implemented functions, ports, protocols, and services. f) The Contractor uses a process to identify the components authorized to execute on LSRMS, and employs a deny-all, permit-by-exception policy to allow the execution of authorized components on the information system; and reviews and updates the list of authorized components	
SR-37	Configuration Management	The Contractor should develop, document, and maintain an inventory of the LSRMS components that: a) Accurately reflects their current configuration; b) Is at the level of granularity deemed necessary for tracking and reporting; c) Includes enough information to achieve effective property accountability; d) Is available for review and audit by TB; and e) Is updated as an integral part of component installations, removals, and LSRMS updates.	CM-8, CM-8(1)
SR-38	Configuration Management	The Contractor should provide a LSRMS Configuration Management Plan that: a) Addresses roles, responsibilities, and configuration management processes and procedures b) Defines the Configuration Items for LSRMS and when the Configuration Items are placed under configuration management; c) Establishes the means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items; d) Defines the processes for patch management on custom software utilized within the LSRMS Infrastructure that includes: i. Identifying, reporting, and correcting flaws in custom software; ii. Testing software updates related to flaw remediation for effectiveness and potential side effects on the LSRMS before installation;	CM-9, CM-9(1)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		iii. Incorporating flaw remediation into the LSRMS configuration management process; e) Defines the processes for patch management of the LSRMS Infrastructure components that includes: i. Ensuring the latest version of applications and operating systems are used; ii. Ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; iii. Prioritizing critical patches using a risk-based approach; iv. Taking applications offline and bringing them back online; v. Aligning criticality levels for patches as specified by TB; vi. Rating of vulnerabilities against the Common Vulnerability Scoring System (CVSS v3.0); vii. Testing and verification methodology to ensure that patches have been implemented properly; and viii. Notifying TB of configuration vulnerabilities that would allow an unauthorized individual to compromise the confidentiality, integrity, or availability of LSRMS.	
SR-39	Configuration Management	The Contractor should provide TB with a LSRMS change management process that includes: a) Contractor's change management authorities; b) Contractor resource roles and responsibilities for change management; c) how the Contractor will use the change management process to support the development of the LSRMS (e.g., a concept of operation).	CM-9, CM-9(1)
SR-40	Contingency Planning	(A) The Contractor should develop, document, and disseminate internally and to TB: a) Contingency planning procedures for LSRMS that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b) Procedures to facilitate the implementation of contingency planning controls. (B) The Contractor should review and update the contingency planning procedures at least every year.	CP-1, CP-2

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-41	Contingency Planning	The Contractor should work in conjunction with TB to establish national restoration priorities for LSRMS in an order of precedence as specified by TB.	CP-7, CP-8,
SR-42	Contingency Planning	The Contractor should a) Conduct backups of user-level information contained in the information system (daily incremental; weekly full) b) Conduct backups of system-level information contained in the information system (daily incremental; weekly full) c) Conduct backups of information system documentation including security-related documentation (daily incremental; weekly full) d) Protect the confidentiality, integrity, and availability of backup information at storage locations e) Test the backup data for LSRMS monthly to verify media reliability and data integrity; and f) Use a sample of backup data for LSRMS in the restoration of selected LSRMS functions as part of service continuity plan testing.	CP-9, CP-9(1), CP-9(2)
SR-43	Contingency Planning	The Contractor should store backup copies of operating system software, critical system software, and component inventory in a separate facility or fire-rated container that is not collocated with the LSRMS Infrastructure.	CP-9(3)
SR-44	Contingency Planning	The Contractor should restore the LSRMS to a known state after a disruption, compromise, or failure.	CP-10
SR-45	Identification and Authentication	a) The Contractor should provide TB with the operational security procedures that includes operational roles and responsibilities for identification and authentication requirements to be defined in the tailoring process. b) The Contractor should review and update the identification and authentication procedures at least annually.	IA-1

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-46	Identification and Authentication	The LSRMS should a) uniquely identify and authenticate Operators (or processes acting on behalf of Operators). b) issue user name and password credentials for Accounts that comply with the requirements for Level 3 Assurance as described in ITSP.30.031 V3 c) allow challenge/response questions for password recovery; d) allow one-time temporary passwords for enrolment and password recovery; e) allow one-time temporary passwords that are sufficiently random so as to not be predictable and with a configurable validity period as specified by TB; f) allow automatic advanced notification of pending password expiry as specified by TB; g) allow password recovery policies and processes; and h) authenticate all Software Client access to the LSRMS.	IA-2
SR-47	Identification and Authentication	The LSRMS should enforce multifactor authentication for network access to privileged accounts.	IA-2(1)
SR-48	Identification and Authentication	The LSRMS Infrastructure should a) enforce multi-factor authentication using hard crypto token for all Operator accounts in compliance with an LoA4 assurance level, as detailed in ITSP.30.031 V3 (https://www.cse-cst.gc.ca/en/node/1842/html/26717); and b) perform mutual authentication of Operators Portable Devices connected to the network and only accept authorized Operators Portable Devices. Authorized portable data storage devices should be password (entered directly on device) or biometric controlled and all information stored on them should be should be encrypted using a *Cryptographic Module Validation Program* certified encryption module running on the storage device itself.	IA-3, IA-3(1), CSE ITSG-33 Specific: IA-2(100)
SR-49	Identification and Authentication	The Contractor should manage LSRMS Infrastructure Operators accounts by: a) identifying account types (i.e., individual, group, system, device, application, guest/anonymous, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the LSRMS Infrastructure and specifying access privileges;	IA-4

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		d) requiring appropriate approvals for requests to establish accounts; e) selecting an identifier that uniquely identifies the Operator or device; f) assigning the Operator identifier to the intended party or the device identifier to the intended device; g) establishing, activating, modifying, disabling, and removing accounts; h) specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; i) notifying account administrator when temporary accounts are no longer required and when LSRMS Infrastructure Operators are terminated, transferred, or LSRMS Infrastructure usage or need-to-know/need-to-share changes; j) preventing reuse of identifiers for at least one year; k) deactivating: i. Temporary accounts that are no longer required; ii. Accounts of terminated or transferred Operators; iii. Accounts after a number of day of inactivity as specified by TB, and iv. Temporary and emergency accounts over a given age; l) Granting access to the LSRMS Infrastructure based on: i. A valid access authorization; ii. Intended system usage, and iii. Other attributes as required by the Contractor or TB; m) Reviewing accounts at least monthly; n) Locking the account after 10 unsuccessful login attempts occurring within 5 minutes, and o) Keeping the account locked until manually unlocked by another Operator. The Contractor should provide mechanisms to: a) Prevent reuse of identifiers for User accounts (no time limit); and b) Disable User account identifiers after defined time periods of inactivity (for each User account type) to be determined by TB.	

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33

SR-50	Identification and Authentication	The LSRMS Identification Credential and Access Management service should log the following events:
		a) account creation;
		b) account modifications
		c) account disabling,
		d) account termination;
		e) password changes;
		f) credential registrations;
		g) password recovery;
		h) expired credentials
		The LSRMS Identification Credential and Access Management service should protect the audit log with access controls and a tamper-detection mechanism that detects unauthorized modifications to the log data (e.g., by using digital signatures).
			AU-2(3),
			IA-4

SR-51	Identification and Authentication	The Contractor should manage user authenticators for Operators by: a) Verifying, as part of the initial authenticator distribution, the identity of the individual receiving the authenticator; b) Establishing initial authenticator content for authenticators defined by the contractor; c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; d) Establishing and implementing administrative procedures for initial authenticator distribution, lost/compromised or damaged authenticators, and revoking authenticators; e) Changing default content of authenticators upon LSRMS infrastructure component installation; f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) Changing/refreshing authenticators at a frequency not exceeding 180 days; h) Protecting authenticator content from unauthorized disclosure and modification, and i) Requiring operators to take specific measures to safeguard authenticators.	IA-5
SR-52	Identification and Authentication	The LSRMS authentication process for X.509 credentials should include: a) Performing path validation of the X.509 certificate; and b) Checking the revocation status of the X.509 certificate.	IA-5

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-53	Identification and Authentication	The LSRMS Infrastructure must, for password-based authentication: a) enforce minimum password complexity of case sensitive, 15 characters, with at least one upper case, one lower case, one number, and one special character; b) encrypt passwords in transmission; c) hash passwords in storage; d) enforce password maximum lifetime of 90 days, and e) prohibit password reuse for 10 generations.	IA-5(1)
SR-54	Identification and Authentication	The LSRMS Identity Credential and Access Management Service should provide a) the User with a checklist that presents the rules a password should comply with and check these rules positively as they are satisfied when the User enters the password. b) configurable User password rules as specified by TB that include: i. Minimum number of total characters; ii. Minimum number of uppercase and lowercase characters; iii. Minimum number of numeric characters; iv. Minimum number of non-alpha-numeric characters; v. Words found in dictionary (English and French); vi. Password re-use history; and vii. Maximum lifetime of the password.	IA-5(1)
SR-55	Identification and Authentication	The Contractor should require that the registration process for LSRMS Operators to receiver identifiers and authenticators be carried out in person before a designated registration authority with authorization by a designated Contractor's official (e.g., a supervisor).	IA-5(3)
SR-56	Identification and Authentication	The LSRMS Infrastructure should not transmit clear text passwords over any network.	IA-5(6)
SR-57	Identification and Authentication	The Contractor should not allow unencrypted static authenticators to be embedded in LSRMS Infrastructure applications or access scripts or stored on function keys.	IA-5(7)
SR-58	Identification and Authentication	The LSRMS Infrastructure should obscure feedback of Operator or User authentication data (e.g., masking password fields) during the authentication process.	IA-6

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-59	Identification and Authentication	The Contractor should establish a process for maintenance personnel authorization that includes: a) Maintaining a current list of authorized maintenance organizations or personnel; b) Ensuring that personnel performing maintenance on the TB LSRMS have required access authorizations, and c) Having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.	IA-8
SR-60	Incident Response	The Contractor should: a) provide TB with the operational security procedures that includes operational roles and responsibilities for Incident response requirements to be defined in the tailoring process.	IR-1
SR-61	Incident Response	The Contractor should: a) provide a service continuity plan (SCP) that includes operational roles and responsibilities for ensuring continuity of service. b) test the service continuity plan (all processes, procedures, roles, responsibilities etc.) on an annual basis, and provide the test results to TB within 10 Federal Government Working Days of completion of the service continuity plan testing. c) provide the SCP to TB that includes: i. Detailed plan and documented processes for restoring LSRMS; ii. Details the communications plan with TB and its suppliers; iii. Details plan and processes for transferring operational, management and administration functionality to a backup operations centre; iv. Back up strategies for datacenter facilities, network facilities, operational support systems and data, and key service components; v. How the Contractor will ensure that its suppliers have in place service continuity plans; vi. Describes the process for testing the Service Continuity Plan; vii. Steps the Contractor will take if any of its key suppliers go out of business, and	

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		viii. Steps the Contractor will take if any of its manufacturers or Original Equipment Manufacturers (OEM) is no longer considered a trusted manufacturer or OEM by TB.	
SR-62	Incident Response	The Contractor should provide a final version of the Service Continuity Plan within 15 Federal Government Working Days after receiving comments from TB on the draft Service Continuity Plan.	
SR-63	Incident Response	The Contractor should implement the Service Continuity Plan (all processes, procedures, roles, responsibilities etc.), and any subsequent annual updates, within 60 Federal Government Working Days following acceptance by TB.	
SR-64	Incident Response	The Contractor should provide to TB within 40 Federal Government Working Days of a request, evidence not greater than 12 months old, (e.g. test results, evaluations, and audits, etc.) that the Service Continuity Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting TB's service continuity requirements.	
SR-65	Incident Response	If the Contractor determines that it will take more than 40 Federal Government Working Days to provide the requested evidence for the Service Continuity Plan, the Contractor should notify TB within 5 Federal Government Working Days of the original request for evidence, and request an extension, in writing with appropriate justification. Granting an extension is within TB's sole discretion.	
SR-66	Incident Response	The Contractor should respond to security alerts, advisories, and directives from designated external organizations, approved by TB, on an ongoing basis including: a) Constantly monitoring security alerts, advisories, and directives; b) Generating internal security alerts, advisories, and directives as deemed necessary or as directed by TB; c) Disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) Implementing security directives in accordance with established time frames, or notifies TB of the degree of non-compliance.	IR-1, IR-4, IR-6, IR-8, SI-5, SI-5(1)
SR-67	Incident Response	In addition to any sources of intelligence on cyber threats and Incidents sources that the Contractor monitors in its routine operations, the Contractor should monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC)	IR-1, IR-4, IR-8

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		(https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx).	
SR-68	Incident Response	The Contractor should provide a Security Operations Centre (SOC), prior to the completion of operational readiness phase, with the infrastructure and resources required for the centralized monitoring and resolution (24 hours per day, 7 days per week, 365 days per year) of LSRMS Security Incidents.	IR-1
SR-69	Incident Response	The Security Operations Center (SOC) should: a) Coordinate Security Incident response in close coordination with TB; b) Include a unique and dedicated telephone number available 24 hours per day, 7 days per week, 365 days per year answered using the official language of Canada (French, English) as requested by the caller; c) Act as a point of contact for communications with TB representatives for security incidents; d) Not impact operations of LSRMS in case of a Contractor Security Operations Center (SOC) failure; e) Notify TB within 15 minutes if Contractor SOC is not available and provide contact name TB can communicate as necessary during the Contractor SOC outage.	IR-1, IR-4 IR-5, IR-6, IR-8
SR-70	Incident Response	The SOC should work with SSC's Information Protection Centre (IPC) for activities that include: a) Integration of processes; b) Oversight; c) Security incident handling and response; d) Auditing; e) Security Incident containment, eradication and recovery that include: i. Ability to dispatch the IT Security Incident Recovery Team (ITSIRT) to the Contractor site; and ii. Allowing TB to provide on-site guidance and coordination.	IR-1

SR-71	Incident Response	The Contractor should automatically provide Incident Ticket information by secure e-mail to pre-defined distribution lists for each Incidents where TB specifies:
		a) Information from Incident Ticket;
		b) Frequency of updates;
		c) Distribution lists, and
			IR-1,
			IR-2,
			IR-4,
			IR-5,
			IR-6,
			IR-8

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		d) Criteria for selecting Incidents (severity, priority, content of Incident Ticket).	
SR-72	Incident Response	The Contractor should continue to automatically send secure e-mail upon updates of Incidents until the Incident is closed or TB cancels the automatic update reporting for the Incident.	IR-1, IR-2, IR-4, IR-5, IR-6, IR-8
SR-73	Incident Response	The Contractor should implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious malware) to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by TB authorized representatives, as specified by TB in accordance with Canada's priority level.	IR-1, IR-2, IR-6

SR-74	Incident Response	The Contractor should provide a Security Incident post-mortem report to TB, within 72 hours of a request by TB, that includes, but is not limited to:
		a) Security Incident number;
		b) Security Incident opened date;
		c) Security Incident closed date;
		d) description of Security Incident;
		e) scope of Security Incident;
		f) chain of events / timeline;
		g) actions taken by Contractor;
		h) lessons learned;
		i) limitations/issues with LSRMS, and
		j) recommendations to improve LSRMS.
			IR-1,
			IR-2,
			IR-4,
			IR-5,
			IR-6,
			IR-8

SR-75	Incident Response	The Contractor should monitor on a continuous basis events on the LSRMS Infrastructure to: a) detect attacks, Incidents and abnormal events against the LSRMS and the Infrastructure; b) identify unauthorized use and access of LSRMS Data and LSRMS Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the LSRMS.	IR-1, IR-2, IR-4, IR-5, IR-6, IR-8
SR-76	Incident Response	The Contractor should provide training for LSRMS Infrastructure Operators in their security Incident response roles and responsibilities and provide annual refresher training.	IR-2
SR-77	Incident Response	The Contractor should test the Incident response process for the LSRMS at least annually using comprehensive test scripts to determine the Incident response effectiveness including:	IR-3

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		a) documenting the test results; b) reviewing the test results with TB, and c) implement corrective actions as required by TB within a timeframe agreed to with TB.	
SR-78	Incident Response	The Contractor should ensure that the security posture of the LSRMS is maintained by continuously: a) monitoring threats and vulnerabilities; b) monitoring for malicious activities and unauthorized access; and c) where required, taking proactive countermeasures, including taking both pre-emptive and response actions to mitigate threats.	IR-4
SR-79	Incident Response	The SOC should a) accept e-mails from TB authorized representatives to a Contractor-provided mailbox with an auto reply to confirm receipt of the e-mail; b) acknowledge receipt of e-mails received from LSRMS addresses authorized by TB within 15 minutes of receiving the e 24 hours per day, 7 days per week, and 365 days per year; c) authenticate the identity of the requester using a process approved by TB.	IR-4
SR-80	Incident Response	The Contractor should create one or more Incident Tickets for each Incident detected by the Contractor or reported by TB.	IR-4
SR-81	Incident Response	The Contractor should physically and/or logically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket should be recorded in TB dedicated storage.	IR-4
SR-82	Incident Response	The Contractor should open an Incident Ticket within 5 minutes of notification for both Contractor-determined and TB-reported Incidents.	IR-4
SR-83	Incident Response	The Contractor should review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing/exercises.	IR-4
SR-84	Incident Response	The Incident Tickets for Security Incidents should include, the following additional information: a) Type and description of attack/event; b) Whether attack appears to have been successful and impact; c) Attack scope;	IR-5

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33

		d) Estimated number of systems and system components affected;
		e) List of systems and system components affected by organization;
		f) Apparent source/origin of attack/incident/event;
		g) Date/time of attack/incident/event;
		h) Estimated injury level /sector;
		i) Estimated impact level;
		j) Attack/incident/event duration;
		k) Actions taken;
		l) Status of mitigations, and
		m) Applicable logs or evidence data.	

SR-85	Incident Response	The Contractor should report all suspected or actual privacy and security violations for LSRMS as Security Incidents.	IR-6
SR-86	Incident Response	The Contractor should provide all evidence, in a COTS format specified by TB, associated to a Security Incident, within a time interval specified by TB that includes: a) Logs and audit records based on criteria provided by TB, and b) Additional information or data as specified by TB.	IR-6
SR-87	Incident Response	The Contractor should open an Incident Ticket within 5 minutes of notification for both Contractor-determined and TB-reported Incidents.	IR-6
SR-88	Incident Response	The Contractor should update the Incident within 5 minutes of a change in status of a high priority Incident and within 15 minutes of a change in status of all other Incidents.	IR-6

SR-89	Incident Response	The Contractor's Incident Tickets should include and maintain, but not be limited to, the following dedicated information fields for all Incidents:
		a) Contractor's Ticket number;
		b) Incident description;
		c) Incident originator contact information (name, telephone number and LSRMS identifier);
		d) Incident originator language;
		e) Related Incident Tickets;
		f) Date and time stamp when Incident Tickets initiated;
		g) Date and time stamp when Incident Ticket closed;
		h) Incident Ticket type; type (e.g. production, functional testing, performance testing, security, etc.) as specified by TB;
		i) Incident Ticket severity;
		j) Incident Ticket impact;
		k) Incident Ticket priority;
			IR-6

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33

		l) Incident Ticket status (i.e. open, closed, in progress, suspended, cancelled etc.);
		m) Incident Ticket escalations;
		n) TB's ticket number;
		o) Service functions impacted;
		p) Affected Service Delivery Points;
		q) Contractor contact (name, telephone number and LSRMS identifier);
		r) Partner identifier (If applicable);
		s) Interactions with third parties;
		t) Activity log;
		u) Root cause (if available);
		v) Estimated time for resolution (updated every 15 minutes);
		w) Resolution description and
		x) Outage time (for closed tickets only).	

SR-90	Incident Response	The Contractor should open an Incident Ticket within 5 minutes of notification for both Contractor-determined and TB-reported Incidents.	IR-6
SR-91	Incident Response	The Contractor should update the Incident within 5 minutes of a change in status of a high priority Incident and within 15 minutes of a change in status of all other Incidents.	IR-6
SR-92	Incident Response	The Contractor should notify TB via phone and LSRMS (7 days x 24 hours x 365 days), based on priority as specified by TB, of any suspected or actual Security Incidents, including but not limited to: a) Ransomware attacks; b) Denial of service attacks; c) Malware; d) Social engineering; e) Unauthorized intrusion or access; f) Information breach; and g) All other security breaches or cyber threats targeting Canada.	IR-6
SR-93	Incident Response	The Contractor should not withhold from TB any information or data in its possession that relates to LSRMS or is associated with a Security Incident.	IR-6
SR-94	Incident Response	The Contractor should provide a secure Security Management Portal that will allow Canada to view security-related information within the LSRMS. This includes but is not limited to: a) Security Incident reports, post-mortem, adhoc reports, and associated evidence;	IR-6

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33

		b) Security Incident tickets;
		c) User activity reports;
		d) Operator activity reports;
		e) Access reports;
		f) Configuration audit reports;
		g) Configuration change reports;
		h) File integrity monitoring reports;
		i) Inventory reports;
		j) Vulnerability reports;
		k) Configuration change reports;
		l) Emergency Request for Changes and Request for Changes;
		m) Patches and security patches implemented;
		n) Information on whether specific LSRMS users are being blocked/filtered and for how long; and
		o) Other supporting documentation (e.g. whitelisting, blacklisting).	

SR-95	Incident Response	The Contractor should report all suspected or actual privacy and security violations for LSRMS as Security Incidents.	IR-6
SR-96	Incident Response	Meetings for Security Incidents, or security related matters as identified by TB, should be in Person in the National Capital Region (NCR) during regular business hours (08:00 to 17:00 ET) Monday to Friday and during hours outside that time period as agreed to between the Contractor and TB.	IR-7(2)
SR-97	Incident Response	The Contractor should be available to participate in a Security Incident briefing provided by Canada.	IR-7(2)
SR-98	Incident Response	The Contractor should have proper forensic procedures and safeguards in place that includes: a) The maintenance of a chain of custody for both the audit information, and b) The collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.	IR-8
SR-99	Incident Response	The Contractor should develop an incident response plan that includes: how the Contractor plans to identify, report, and escalate Security Incidents; a) A roadmap for implementing the Security Incident response capability that includes preparation, detection, analysis, containment and recovery; b) A description of the structure and organization of the Security Incident response capability;	IR-8

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		c) A high-level approach for how the Security Incident response capability fits into the Contractor's overall organization; d) A definition of reportable Security Incidents; e) A definition of metrics for measuring the Security Incident response capability; and f) A definition of resources and management support needed to effectively maintain and mature the Security Incident response capability.	
SR-100	System Maintenance	The Contractor should perform controlled maintenance by: a) Scheduling, performing, documenting, and reviewing records of maintenance and repairs on LSRMS Infrastructure components in accordance with manufacturer or vendor specifications; b) Controlling all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location; c) Requiring that a designated Contractor's official explicitly approve the removal of the LSRMS Infrastructure components from the Contractor data centre for off-site maintenance or repairs; d) Sanitizing equipment to remove all data from associated media prior to removal from Contractor's facilities for off-site maintenance or repairs, and e) Checking all potentially impacted security requirements to verify that the controls are still functioning properly following maintenance or repair actions.	MA-2, MA-2(1), MA-2(2)
SR-101	System Maintenance	The Contractor should approve, control, monitor and maintain, on an ongoing basis, the hardware and software used for maintaining the LSRMS Infrastructure specifically for diagnostic and repair actions (e.g., a hardware or software tools that are introduced for the purpose of a particular maintenance activity).	MA-3
SR-102	System Maintenance	The Contractor should a) Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications ; b) Check all media containing diagnostic and test programs for malicious code before the media are used on LSRMS Infrastructure components;	MA-3(2), MA-3(3), MA-3(4)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		c) Prevent the unauthorized removal of maintenance equipment containing LSRMS information by: i. Verifying that there is no LSRMS information contained on the equipment; ii. Sanitizing or destroying the maintenance equipment; iii. Retaining the equipment within the LSRMS facility or obtaining an exemption from a designated LSRMS Contracting Authority explicitly authorizing removal of the equipment from the LSRMS facility. d) Restrict the use of maintenance tools to authorized personnel only.	
SR-103	System Maintenance	The Contractor should authorize, monitor, and control maintenance and diagnostic activities on the LSRMS Infrastructure by: a) Allowing the use of maintenance and diagnostic tools approved by TB; (to be discussed) b) Employing strong identification and authentication techniques in the establishment of maintenance and diagnostic sessions that are tightly bound to the user and by separating the maintenance session from other network sessions with the LSRMS Infrastructure by either: i. Physically and/or logically separated communications paths; or ii. Logically separated communications paths using CSE-approved cryptographic modules and algorithms; c) Recording maintenance and diagnostic sessions; and d) Having designated personnel review the records of the maintenance and diagnostic sessions.	MA-4, MA-4(1)
SR-104	System Maintenance	The Contractor should establish a process for maintenance personnel authorization that includes: a) Maintaining a current list of authorized maintenance organizations or personnel; b) Ensuring that personnel performing maintenance on the LSRMS have required access authorizations, and c) Having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.	MA-5

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-105	Media Protection	The Contractor should provide TB with the operational security procedures that include media protection requirements to be defined in the tailoring process.	MP-1
SR-106	Media Protection	The Contractor a) Should restrict access to IT media (digital and non-digital) containing LSRMS Data to authorized Operators; and b) Employ mechanisms to audit access attempts and access granted.	MP-2, MP-2(1)
SR-107	Media Protection	The Contractor should mark, in accordance with the provisions of the contract, removable IT media containing Canada information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	MP-3
SR-108	Media Protection	The Contractor should a) Physically and/or logically control and securely store IT media containing LSRMS Data in accordance with the RCMP G1-001, Security Equipment Guide; and b) Protect media containing LSRMS data until the media are destroyed or sanitized using approved equipment, techniques, and procedures (as per CSE's Clearing and Declassifying Electronic Data Storage Devices (ITSG-06)).	MP-4
SR-109	Media Protection	The Contractor should employ cryptographic mechanisms to protect LSRMS information in storage that are approved by TB and are in compliance with CSE guidance (ITSP.40.111).	MP-4(1)
SR-110	Media Protection	The Contractor should sanitize and verify IT media containing LSRMS Data, both digital and non-digital, prior to disposal, release out of the Contractor's control, or release for reuse.	MP-6, MP-6(1)
SR-111	Media Protection	The Contractor must track, control and verify media sanitization by: a) Performing media sanitization in compliance with ITSG-06 (https://www.cse-cst.gc.ca/en/node/270/html/28460) requirements for Protected B information; b) Recording media sanitization actions; c) Testing sanitization equipment and procedure to verify correct performance at least annually; and d) Sanitizing re-allocated used storage devices prior to connecting them to the TB LSRMS Infrastructure	MP-6(2), MP-6(3), MP-6(4), MP-6(5), MP-6(6)
SR-112	Physical and Environmental Protection	The Contractor should provide TB with the operational security procedures that includes physical and environmental	PE-1

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		protection requirements to be defined in the tailoring process.	
SR-113	Physical and Environmental Protection	The Contractor should implement role-based physical access control to its LSRMS Infrastructure facilities including: a) Keeping an access list of personnel with authorized access to the facilities; b) Issuing authorization credentials for access to the facilities; c) Reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access; d) Authorizing physical access to the facilities, by access point, based on the role of the individual; e) Adjust role assignment as Operator role changes to new role; f) Implementing separation of duties where the authorization to access facilities is done by a different person than the person doing the authorization to access the LSRMS Infrastructure; g) Allowing access to facilities to authorized personnel based on a need-to-know and need-to-access; h) Keeping the management of the Contractor's physical access control authorizations to the LSRMS Facility independent of the physical access control authorization to the facility where the LSRMS Facilities are located; and i) If emergency access is required, contact the RCMP for advice.	PE-2, PE-2(1), PE-2(2), PE-2(3) CSE ITSG 33 Specific: PE-2(100), PS-5
SR-114	Physical and Environmental Protection	The Contractor should provide TB with a building security plan for review by TB including: a) Physical security layout for access control points; b) Physical security zones; c) Monitoring physical access points; and d) The Contractor should enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the infrastructure resides (excluding those areas within the facility officially designated as publicly accessible); i. Verify individual access authorizations before granting access to the facility;	PE-3, PE-3(1), PE-3(2) PE-3(3), PE-3(4), PE-3(5), PE-3(6), PE-4, PE-5

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		ii. Controls entry to the facility containing the infrastructure using physical access devices and/or guards; iii. Control access to areas officially designated as publicly accessible in accordance with the Contractor's assessment of risk; iv. Secure keys, combinations, and other physical access devices; v. Inventories physical access devices at least annually; and vi. Combinations and keys should be changed immediately when keys are lost, combinations are compromised, or individuals are transferred or terminated.	
SR-115	Physical and Environmental Protection	The Contractor should monitor physical access to LSRMS Infrastructure facilities by: a) Monitoring in real-time physical intrusion alarms and surveillance equipment; b) Recording all physical access events; c) Reviewing physical access logs at least monthly; d) Providing logs on a monthly basis and as requested by TB; and e) Create a Security Incident upon discovery of abnormal activity.	PE-6, PE-6(1), PE-6(2)
SR-116	Physical and Environmental Protection	The Contractor should control physical access to LSRMS Infrastructure facilities by: a) Authenticating visitors before authorizing access with TB approval to the facility where the infrastructure resides; b) Authenticating visitors with two forms of identification prior to granting access to the LSRMS facility; and c) Escorting visitors and monitoring visitor activity, within the LSRMS Facility at all times.	PE-7, PE-7(1), PE-7(2)
SR-117	Physical and Environmental Protection	The Contractor should authorize, monitor, and control all components entering and exiting the LSRMS Infrastructure facilities and maintain records of those components and activities. Records should be made available monthly and as requested by GC.	PE-16
SR-118	Physical and Environmental Protection	The Contractor should a) Implement at alternate work sites management, operational, and technical security controls that	PE-17, PS-1

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		achieve the same objectives as those implemented at the main LSRMS Facility. b) Alternate site should be approved concurrently with the Primary sites by CISD/IISD.	
SR-119	Personnel Security	The Contractor should, upon termination of an individual's employment associated with LSRMS: a) Terminate physical access to LSRMS Infrastructure facilities for the employee; b) Terminate LSRMS Infrastructure access, including remote access, and c) Retrieve all security-related property (e.g., employee identity card, physical authentication token).	PS-4
SR-120	Personnel Security	The Contractor should manage LSRMS Infrastructure Privileged Operators accounts as follows: a) Create Operator accounts in accordance with role-based access profiles that specify privileges; b) Track and monitor Operator role assignments, and c) Adjust role assignments as Operator role changes.	PS-5
SR-121	Personnel Security	The Contractor should have access agreements to the LSRMS Infrastructure or LSRMS Data. The Contractor should ensure that Operators requiring access to organizational information and information systems: a) Sign appropriate access agreements prior to being granted access; and b) Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated. The Contractor reviews and updates access agreements to the LSRMS Infrastructure or LSRMS Data every two years.	PS-6
SR-122	Personnel Security	The Contractor should a) Ensure that the Operators sign an access agreement (prior to being granted access to the LSRMS Infrastructure or LSRMS Data) that list the formal sanctions process for failing to comply with the terms and conditions of the access agreement, and b) Provide training for LSRMS Infrastructure Operators in their responsibilities to protect the privacy and confidentiality of the LSRMS Data as per the terms and conditions of the LSRMS contract and in the sanctions for failure to comply. The Contractor should provide bi-annual refresher training.	PS-8

Security Requirement IDs (for Canada's purpose only)	**Requirement Category**	**Description**	**ITSG-33**
SR-123	Risk Assessment	The Contractor should allow TB, or its representatives, to conduct a Vulnerability Assessment against the LSRMS, within 3 Federal Government Working Days of a request by TB, that includes: a) Physical access to the LSRMS facilities (i.e. Contractor's facilities where the LSRMS Infrastructure (i.e. hardware and software) is located); b) Network access(es) to the LSRMS Infrastructure to allow for authenticated and unauthenticated scanning of network components and security appliances, using TB operated equipment, and TB specified tools; c) Assistance for the duration of any onsite portion of the vulnerability assessment of at least one technical resource that is familiar with the technical aspects of the LSRMS Infrastructure (i.e., the hardware, software, and network components, security appliances, and their configuration); d) TB will limit its Vulnerability Assessment to discovery and scanning activities to LSRMS Infrastructure and will not engage in disruptive or destructive activities.	RA-5
SR-124	System and Services Acquisition	From the date vulnerabilities are formally identified, the Contractor should, at a minimum: a) Mitigate all high-risk vulnerabilities within 10 days; and b) Mitigate all moderate risk vulnerabilities within 30 days. TB and Contractor will mutually agree and determine the risk rating of vulnerabilities. The Contractor should: a) Incorporate information security considerations when developing, customizing or modifying LSRMS. b) Define and document information security roles and responsibilities throughout the system development life cycle. c) Identify individuals having information security roles and responsibilities. d) Integrate the organizational information security risk management process into system development life cycle activities.	SA-3

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-125	System and Services Acquisition	The Contractor should maintain the LSRMS security authorization state through continuous monitoring and annual audit of the implemented security requirements within the LSRMS to determine if the security requirements in the information system continue to be effective over time in light of changes that occur in the LSRMS and its operational environment.	SA-3
SR-126	System and Services Acquisition	The Contractor should provide evidence to support security authorization maintenance activities, within 30 days of a request by TB, following all changes to the LSRMS Infrastructure within the Contractor's control.	SA-3
SR-127	System and Services Acquisition	The Contractor should update, as requested by TB, and within 30 days of a request by TB, security operating procedures and demonstrate implementation as part of authorization maintenance.	SA-3
SR-128	System and Services Acquisition	The Contractor must restrict the location of information processing, information/data, and information system services to Canada.	SA-9 (5)
SR-129	System and Communications Protection	The Contractor as part of the Security Operational Procedures must include policy and procedures to facilitate the implementation and maintenance of the system and communications protection requirements and in applicable GC standards to be defined in the tailoring process.	SC-1
SR-130	System and Communications Protection	The LSRMS should include a capability to protect against Denial of Service (DoS) attacks that limits concurrent connections as specified by TB.	SC-5, SC-5(1), SC-5(2)
SR-131	System and Communications Protection	1. The service design for LSRMS should conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 and ITSG-38.Additionally, The LSRMS Infrastructure should monitor and control communications at the external boundary of the system and at key internal boundaries within the system in compliance with ITSG-22 and ITSG-38. 2. The LSRMS Contractor should monitor and analyze network traffic, in near real time, to detect attacks and evidence of compromised LSRMS Infrastructure components. 3. The LSRMS Contractor should detect attacks including but not limited to: i. Ransomware attacks; ii. Denial of service attacks; iii. Malware;	SC-7

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		iv. Social engineering; v. Unauthorized intrusion or access; vi. Information breach; and vii. All other security breaches or cyber threats targeting Canada.	
SR-132	System and Communications Protection	The LSRMS Infrastructure should exclusively connect to external networks or information systems specified by Canada only through managed interfaces specified by Canada using boundary protection devices arranged in compliance with ITSG-22 and ITSG-38.	SC-7(2)
SR-133	System and Communications Protection	The Contractor should actively manage all network connections to external services associated with the LSRMS Infrastructure as follows: a) Deny all network traffic by default; b) Define allowable traffic for each network connection (i.e. Deny all, permit by exception); c) Terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by TB; d) Document each exception to the traffic flow policy with a supporting need and duration of that need; e) Review exceptions to the traffic flow policy at least annually; f) Remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) Monitor traffic for unusual or unauthorized activities or conditions; and h) As necessary, monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.	SC-7(4), SC-7(5)
SR-134	System and Communications Protection	The Contractor should prevent Contractor managed devices (e.g.: notebook or other device used for administration) that are connected with the LSRMS Infrastructure from communicating outside of that communications path (e.g. accessing the Internet via a separate connection available to the device).	SC-7(7)
SR-135	System and Communications Protection	The LSRMS Infrastructure should detect extrusion events in near real time.	SC-7(9)
SR-136	System and Communications Protection	The Contractor should monitor and analyze hosts behaviours (Host-based Intrusion Detection and Prevention) in **near real-time** to detect attacks and evidence of compromised hosts	SC-7(12)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-137	System and Communications Protection	The Contractor should **Physically and/or logically** separate the network IP traffic a) Of the LSRMS System Data from the LSRMS Management Data and LSRMS User Data. b) Between the LSRMS Management Data and the LSRMS User Data.	SC-7(13)
SR-138	System and Communications Protection	The Contractor should configure boundary protections (i.e. firewall) to fail safe (i.e. no traffic goes through) upon failure.	SC-7(18)
SR-139	System and Communications Protection	The LSRMS Design must: a) Allow mutual authentication of connections, between the LSRMS and other domains as specified by TB, and exclusively exchange information with these other domains using mutual authentication; and b) Ensure that the integrity and confidentiality of LSRMS Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by TB.	SC-8
SR-140	System and Communications Protection	The LSRMS Infrastructure must protect the integrity and confidentiality of LSRMS Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms, unless otherwise protected by alternative physical measures approved by TB.	SC-8(1)
SR-141	System and Communications Protection	The LSRMS Design must: a) Allow mutual authentication of connections, between the LSRMS and other domains as specified by TB, and exclusively exchange LSRMS Messages with these other domains using mutual authentication; b) Ensure that the integrity and confidentiality of LSRMS Data during transmission and at rest is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by TB; c) Conform to network security zoning in accordance with ITSG-22 and ITSG-38; and d) Encrypt Security Incident information with approved cryptographic standards if the information is sent in electronic form.	SC-9, SC-9(1), SC-9(2), SC-12(1), SC-12(2), SC-12(3), SC-12(4), SC-12(5), CSE ITSG-33 Specific: SC-9(100)
SR-142	System and Communications Protection	The LSRMS Design should ensure that cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for LSRMS: a) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSE and validated by the Cryptographic Algorithm	SC-13, CSE ITSG-33 Specific: SC-13(100), SC-13(101)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		Validation Program, and are specified in ITSP.40.111 (https://www.cse-cst.gc.ca/en/node/1831/html/26515); b) Be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program to at least FIPS 140-2 validation at Level 1, and c) Operate in FIPS Mode.	
SR-143	System and Communications Protection	The Contractor should not prohibit a User to encrypt, decrypt, sign and verify LSRMS attachment files using Certificates trusted by the GC-CA.	SC-17
SR-144	System and Communications Protection	The Contractor should only allow pre-approved mobile code in the LSRMS Infrastructure thus denying any other mobile code from being downloaded and executed.	SC-18, SC-18(1), SC-18(2), SC-18(3), SC-18(4)
SR-145	System and Communications Protection	The LSRMS Infrastructure component or components that collectively provide name/address resolution service for the LSRMS should implement internal/external role separation.	SC-22
SR-146	System and Communications Protection	The LSRMS should allow the authentication of all types of Software Clients with a LSRMS credential.	SC-23
SR-147	System and Communications Protection	The LSRMS Infrastructure must protect the integrity and confidentiality of LSRMS Data during transmission and at rest using Communications Security Establishment -approved cryptographic modules and algorithms unless otherwise protected by alternative physical measures approved by TB.	SC-28
SR-148	System and Communications Protection	The Contractor, at their discretion, can use non-dedicated hardware, non-dedicated software for the operation, administration and management of LSRMS Management Data. Any use of non-dedicated hardware, non-dedicated software is only allowed for LSRMS Management Data according to the following conditions: a) Should not access, process or store LSRMS User Data; b) Should not access, process or store LSRMS System Data; c) should not access, process or store user account names and passwords; d) Should be logically segregated from other client's data; e) Should adhere to all LSRMS Infrastructure requirements outlined in this list of Security Requirements;	SC-32

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		f) Should not access, process or store information labeled as Protected or Classified unless approved in writing by TB; g) Should not access, process or store service design information for the LSRMS; and h) Should not allow for the control or modification of the TB dedicated LSRMS Infrastructure.	
SR-149	System and Communications Protection	The LSRMS should include dedicated controls for any network interconnections between dedicated and non-dedicated LSRMS Infrastructure, according to the approved Security Design, that includes: a) Boundary protection whereby, the Contractor should use current or previously evaluated physical firewall appliances validated under a recognized Common Criteria scheme against an approved Protection Profile that considers firewall evaluation. the Contractor should obtain approval from TB for alternative physical firewall appliances; b) Integration of TB provided threat detection equipment; c) Incorporation of Contractor provided threat detection/prevention solutions; d) Routing of traffic through authenticated proxy servers; and e) Role based access control with least privilege.	SC-32
SR-150	System and Communications Protection	The Contractor should physically and/or logically separate a) Information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket should be recorded in TB dedicated storage; b) Ensure that any network configuration details contained in any asset records and configuration records management systems for the LSRMS Infrastructure are encrypted; c) The network IP traffic of the LSRMS System Data from all other LSRMS Data; and d) Logically separate the network IP traffic between the LSRMS Management Data and the LSRMS User Data.	SC-32
SR-151	System and Communications Protection	The categorization of data for LSRMS as either LSRMS System Data, LSRMS User Data or LSRMS Management Data will be at the sole discretion of TB and based on comparison to other similar data.	SC-32

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
SR-152	System and Information Integrity	The Contractor should provide TB with the LSRMS operational security procedures that includes operational roles and responsibilities for system and information integrity requirements to be defined in the tailoring process.	SI-1
SR-153	System and Information Integrity	The Contractor should define and execute the processes for patch management for the LSRMS Infrastructure components that includes: a) Ensuring the latest version of applications and operating systems are used; b) Ensuring that vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner; c) Prioritizing critical patches using a risk-based approach; d) Taking applications offline and bringing them back online; e) Aligning criticality levels for patches as specified by tb; f) Rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v3.0; and g) Testing and verification methodology to ensure that patches have been implemented properly. h) Defines the processes for patch management on custom software utilized within the LSRMS Infrastructure that includes: i. Identifying, reporting, and correcting flaws in custom software; ii. Testing software updates related to flaw remediation for effectiveness and potential side effects on the LSRMS before installation; and iii. Incorporating flaw remediation into the LSRMS Service configuration management process.	SI-2, SI-2(1), SI-2(2), SI-2(3), SI-2(4)
SR-154	System and Information Integrity	The Contractor should: a) Centrally manage the malicious code protection mechanisms; b) Automatically update malicious code protection/malware mechanisms (including signature definitions) within 6 hours of availability and as requested by TB; c) Prevent non-privileged users from circumventing malicious code protection capabilities;	SI-3(1), SI-3(2), SI-3(3), SI-3(4), SI-3(5)

Security Requirement IDs (for Canada's purpose only)	Requirement Category	Description	ITSG-33
		d) Update malicious code protection mechanisms only when directed by a privileged user; and e) Not allow users to introduce removable media into the LSRMS Infrastructure.	
SR-155	System and Information Integrity	The LSRMS Infrastructure should provide near real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise.	SI-4(5)
SR-156	System and Information Integrity	The LSRMS Infrastructure should prevent all non-privileged users from circumventing intrusion detection and prevention capabilities.	SI-4(6)
SR-157	System and Information Integrity	The Contractor should implement a centrally managed Integrity Verification Solution to detect unauthorized changes to software and LSRMS Infrastructure component configuration including: a) Performing integrity scans at least every 30 days, and b) Automatically generating a Security Incident Ticket upon discovering discrepancies during integrity verification.	SI-7, SI-7(1), SI-7(2)

14.1.2 LSRMS Industry Security Controls

The following are additional security requirements sourced from Cloud Controls Matrix Version 3.0.1, FedRAMP, NIST 800-53, 800-171, and ISO/IEC 27001:

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
SR-158	Data Security & Information Lifecycle Management Data Inventory / Flows	The ***LSRMS Solution*** policies and procedures should be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, Contractor should ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	Tailored based on Industry Best Practices and Departmental Guidance
SR-159	Data Security & Information Lifecycle Management Non-Production Data	The ***LSRMS Solution*** production data should not be replicated or used in non-production environments.	Tailored based on Industry Best Practices and Departmental Guidance
SR-160	Encryption & Key Management Entitlement	The ***LSRMS Solution*** PKI keys must have identifiable owners (binding keys to identities) and there should be key management policies.	Tailored based on Industry Best Practices

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
			and Departmental Guidance
SR-161	Encryption & Key Management Key Generation	The ***LSRMS Solution*** operational policies and procedures must be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, Contractor should inform the TB of changes within the cryptosystem, especially if the LSRMS data is used as part of the service, and/or the TB has some shared responsibility over implementation of the control.	Tailored based on Industry Best Practices and Departmental Guidance
SR-162	Encryption & Key Management Sensitive Data Protection	The ***LSRMS Solution*** operational policies and procedures must be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-User workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Tailored based on Industry Best Practices and Departmental Guidance
SR-163	Encryption & Key Management Storage and Access	The ***LSRMS Solution*** platform and data-appropriate encryption (in compliance with CSE guidance ITSP.40.111) in open/validated formats and standard algorithms must be required. Keys must not be stored in the cloud (i.e. at the LSRMS Cloud Contractor in question), but maintained by the TB or trusted key management Contractor as mutually agreed upon with TB. The LSRMS key management and key usage must be separated duties.	Tailored based on Industry Best Practices and Departmental Guidance
SR-164	Governance and Risk Management Data Focus Risk Assessments	The ***LSRMS Solution*** risk assessments associated with data governance requirements should be conducted at planned intervals as mutually agreed upon with TB and should consider the following: a) Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure;	Tailored based on Industry Best Practices and Departmental Guidance

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		b) Compliance with defined retention periods and end-of-life disposal requirements; and c) Data classification and protection from unauthorized use, access, loss, destruction, and falsification.	
SR-165	Governance and Risk Management Management Oversight	The Contractor's managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Tailored based on Industry Best Practices and Departmental Guidance
SR-166	Governance and Risk Management Management Program	The Contractor should have an Information Security Management Program (ISMP) developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should include, for example the following areas insofar as they relate to the characteristics of the business: a) Risk management b) Security policy c) Organization of information security d) Asset management e) Human resource(s) security f) Physical and environmental security g) Communications and operations management h) Access control i) Information systems acquisition, development, and maintenance	Tailored based on Industry Best Practices and Departmental Guidance
SR-167	Governance and Risk Management Risk Management Framework	All ***LSRMS Solution*** risks should be mitigated to an acceptable level. Acceptance levels based on risk criteria should be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Tailored based on Industry Best Practices and Departmental Guidance
SR-168	Zone Internetwork Device Partitioning	The use of virtual devices in the internetwork zone should be sufficiently partitioned from virtual servers in all zones for infrastructure containing applications of LSRMS.	Tailored based on Industry Best Practices and Departmental Guidance
SR-169	Storage Partitioning	***LSRMS Solution*** storage used by the hypervisor for virtual device images must be physically and/or	Tailored based on Industry

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		logically partitioned for LSRMS infrastructure containing applications of PROTECTED B with MEDIUM injury as defined by TB.	Best Practices and Departmental Guidance
SR-170	Use of Hypervisor Features	The ***LSRMS Solution*** Design Specific Virtual machines should not use any machine to machine sharing mechanism (e.g. file sharing) which is implemented within the hypervisor	Tailored based on Industry Best Practices and Departmental Guidance
SR-171	Hypervisor Certification	The Contractor must use current or previously evaluated hypervisors managing all zones, as defined within the CSE ITSG-22 (https://cse-cst.gc.ca/en/node/268/html/15236) & ITSG-38 (https://cse-cst.gc.ca/en/node/266/html/25034) guidelines, validated under a recognized Common Criteria (https://cse-cst.gc.ca/en/canadian-common-criteria-scheme/main) scheme against an approved Protection Profile that considers hypervisor evaluation for virtual machines protection between zones or obtain approval from TB for alternative products.	Tailored based on Industry Best Practices and Departmental Guidance
SR-172	ICAM	The Contractor’s Interim ICAM Solution should remove all GC User credentials once fully migrated to Canada's GC ICAM solution.	Tailored based on Industry Best Practices and Departmental Guidance
SR-173	Infrastructure & Virtualization Security Management - Vulnerability Management	The Contractor should ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware) within the ***LSRMS Solution***.	Tailored based on Industry Best Practices and Departmental Guidance
SR-174	Infrastructure & Virtualization Security Production / Non-Production Environments	The ***LSRMS Solution*** production and non-production environments must be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: statefull inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties as approved by TB.	Tailored based on Industry Best Practices and Departmental Guidance
SR-175	Infrastructure & Virtualization	Multi-tenant Contractor -owned or managed (physical and virtual) applications, and infrastructure system and network components, should be	Tailored based on Industry Best Practices

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
	Security Segmentation	designed, developed, deployed and configured such that provider and TB (tenant) User access is appropriately segmented from other tenant Users, based on the following considerations: a) Established policies and procedures; b) Isolation of business critical assets and/or sensitive User data, and sessions that mandate stronger internal controls and high levels of assurance; and c) Compliance with legal, statutory and regulatory compliance obligations.	and Departmental Guidance
SR-176	Interoperability & Portability Virtualization	The Contractor should use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and should have documented custom changes made to any hypervisor in use and all LSRMS-specific virtualization hooks available for TB review.	Tailored based on Industry Best Practices and Departmental Guidance
SR-177	Privacy Impact Assessment	As requested by Canada, the Contractor should actively participate in the conduct of a privacy impact assessment on LSRMS in accordance with the *TBS Directive on Privacy Impact Assessmentt* (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308).	Tailored based on Industry Best Practices and Departmental Guidance
SR-178	Physical and Environmental Protection	The Contractor must: a) Screen individuals prior to authorizing access to the information system in accordance with the *TBS Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115)*; b) Rescreen individuals according to conditions requiring rescreening; and c) For Foreign Contractors, *Personnel Screening will be required.*	Tailored based on Industry Best Practices and Departmental Guidance
SR-179	Physical and Environmental Protection	The Contractor must: a) Satisfy the personnel security control requirements including security roles and responsibilities for third-party providers; b) Document personnel security control requirements; c) Monitor provider compliance; d) Ensure security screening of private sector organizations and individuals who have access to Protected information and assets; and	Tailored based on Industry Best Practices and Departmental Guidance

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		e) Explicitly define government oversight and end-user roles and responsibilities relative to third-party provided services.	
SR-180	Physical and Environmental Protection	The Contractor is responsible for recruitment of personnel and the Contractor should: a) Maintain an updated list which clearly identifies personnel by name, title, responsibility, completed training, and b) Facility and systems access levels as set out in the SOW c) Submit the list to the Project Authority when requested. d) Keep an employee record file which can demonstrate that the personnel have the necessary qualifications to perform the work. Such employee record file should be submitted to the Project Authority upon request e) Conduct the following checks as part of the security screening process and provide the information to the Project Authority for each employee upon request: i. Identity check 1. Copies of two of valid original pieces of government issued identity documentation, one of which should include a photo 2. Surname (last name) 3. Full given names (first name) – underline or circle usual name used 4. Family name at birth 5. All other names used (aliases) 6. Name changes (A) Should include the name they changed from and the name they changed to, the place of change and the institution changed through 7. Sex 8. Date of birth 9. Place of birth (city, province/state/region, and country) 10. Citizenship(s)	Tailored based on Industry Best Practices and Departmental Guidance

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		11. Marital status/common-law partnership (A) Current Status (married, common-law, separated, widowed, divorced, single) (B) All current spouses (if applicable) (B1) Surname (last name) (B2) Full given names (first name) – underline or circle usual name used (B3) Date and duration of marriage/common-law partnership (B4) Date of birth (B5) Family name at birth (B6) Place of birth (city, province/state/region, and country) (B7) Citizenship ii. Residency check 12. The last five (5) years of residency history starting from most recent with no gaps in time (C) 1. Apartment number, street number, street name, city, province or state, postal code or zip code, country, from-to dates iii. Educational check 13. The educational establishments attended and the corresponding dates iv. Employment history check 14. The last five (5) years of employment history starting from most recent with no gaps in time 15. Three (3) employment reference checks from the last five (5) years v. Criminal records check: 16. Report(s) containing all criminal convictions for the last five (5) years in and outside of the candidate's country of residence vi. Credit check report where available.	

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		f) Throughout the term of the contract provide the Project Authority with an updated criminal record check and credit g) Check report for all or any personnel upon request, at the Contracting Authority's discretion. h) keep the security screening documentation on file and available to the Contracting Authority for each employee for a i) Period of ten (10) years following the initial offer of employment. j) Rescreens individuals according to conditions requiring rescreening.	
SR-181	Operational Security	The Contractor must: a) Ensure that all activities carried out in relation to the Security and Privacy requirements in the Statement of Work (SOW), provides comparable levels of protection to those identified in GC policies as well as meets or exceeds industry standard or best practice (e.g. ISO 27001), whichever is greater. b) Upon request by the Contracting Authority, provide proof of compliance with legislation in the country of operation which may include, but is not limited to, compliance with national laws concerning privacy protection, adherence to tax laws, incorporation regulations and labour laws. c) Identify an authorized Company Security Officer (CSO) to be responsible for overseeing the privacy and security requirements of Personal Information processed as a result of the Contract. This individual will be the point of contact for privacy and security matters, in collaboration with the Contracting Authority as well as to work with the Contracting Authority for Access to Information (ATIP) requests. The CSO will be accountable for monitoring the application of privacy and security practices and responding to audit comments. Further information on the appointment of and responsibilities of a CSO	Tailored based on Industry Best Practices and Departmental Guidance

Requirement ID	Security Controls	Description	CCM, FedRAMP, NIST, ISO/IEC
		can be found at: https://www.tpsgc-pwgsc.gc.ca/esc-src/ase-cso/roles-eng.html. d) Assign a principal IT security contact with a functional reporting relationship to security management who will ensure that the following functions are performed: i. Establish and manage the Contractor's IT security program as part of the overall security approach; ii. Identify, define and document information system security roles and responsibilities; iii. Make recommendations regarding approval of all contracts for external providers of IT security services; iv. Work with program and service delivery managers to ensure their IT security needs are met, provide advice on safeguards and advise of potential impacts of new and existing threats and on the residual risk of a program or service; v. Monitor departmental compliance with security standards; and vi. Establish an effective process to manage IT security incidents, and monitor compliance	

14.2 Security Traceability Matrix (SRTM)

14.2.1 Acceptable Evidence for Security Control Compliance

This section defines what constitutes acceptable evidence of compliance to the security controls as part of the PSPC SA&A program. PSPC is the final authority on the sufficiency of evidence supplied in support of compliance and the ***LSRMS Solution's*** prime assessor.

14.2.2 Policy, Standards and Guidelines

In order to demonstrate compliance to the security controls which require the Contractor to develop policy, standards or guidelines, the Contractor must in the security control evidence column:

a) Provide the name of the policy instrument where the subject matter is covered.
b) Provide the section reference and page number where the specific subject matter is covered.
c) Provide the policy instrument for PSPC review:
    I. The policy instrument must address all the topics itemized in the security control definition.
    II. The policy instrument must contain a level of detail/coverage consistent with GC policy instruments and industry best practices.

14.2.3 Certification and Clearance

If compliance to the security controls is established through a certification provided by a SubContractor, the Contractor must supply a copy of the certificate and/or the certification report, for example, designated organizational screening: PROT B from PSPC

If compliance to the security controls is established through security clearances for relevant personnel, the Contractor must provide:

a) List of all clearances for relevant personnel,
b) Name of the originating organization for the security clearance, and
c) File number (#), date of issuance, and date of expiry.

14.2.4 Evidence Examples

a) Configuration settings
b) System design documents
c) System architecture or topology diagrams
d) Screenshot of the defined functions
e) Access control lists
f) Configuration management plan
g) Security training and awareness manual
h) Risk register
i) Audit report
j) Vulnerability assessment (VA) report
k) Penetration testing (PenTest) report
l) Business impact assessment (BIA)
m) Title of the contract deliverable(s) for example, IT service continuity and disaster recovery plan
n) Presentations, and
o) Screenshots.

14.2.5 Security Requirement Traceability Matrix Example

Column	Title	Description
1	Sec ID	Unique Security Requirement identifier – for reference and tracking purposes
2	Security Control	Security Control family or name
3	Security Control No.	Security Control number
4	Description	Description of the security control
7	Evidence	Demonstrate compliance to the security controls