INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM) TOOL IMPLEMENTATION SERVICES

ANNEX A

STATEMENT OF WORK (SOW)

RFP Amendment ~~004~~006

Contents

1 INTRODUCTION

1.1 Summary of Requirements

Shared Services Canada (SSC) has established the SSC Service Management Transformation Program that is aimed at fundamentally transforming SSC's Information Technology Service Management (ITSM) capabilities. SSC requires the services of a Contractor to supply, implement and support a complete enterprise class ITSM Tool Solution. The ITSM Tool Solution will be implemented on premise, on SSC provided infrastructure, at Government of Canada (GC) Enterprise Data Centre Services locations.

The Contractor's Work requirements are summarized as follows and more fully described in sections 2 – 13.

a) Contractor Management and Oversight Services	section 2
b) Provision of an Enterprise ITSM Tool including: a. Licensed software to support deployment of ITSM Tool at SSC; b. (optional) Additional licenses to support scaling of the ITSM Tool Solution to SSC customer(s) (as a tenant on the SSC instance or as a separate instance); c. Software Product Documentation; d. Software Upgrades for major releases for the life of the contract; and e. Software Maintenance and Support Services.	section 3
c) Identification of hardware specifications to support SSC provision of the required hardware infrastructure, including: a. Adequate capacity to support Deployment of the Enterprise ITSM Tool at SSC and the initial Tenant Department; and b. Additional capacity to support on-boarding of customers to the ITSM Tool Solution.	section 4
d) Provision of System Integration (SI) professional services required to implement the new ITSM Tool Solution including: a. Contractor On-boarding Requirements; b. Data migration from existing SSC tool(s) to the new Enterprise ITSM Tool; c. Decommissioning strategy of replaced systems and integration; d. Implementation of the Enterprise ITSM Tool (including development of the Functional Design Specifications and configuration of Tool); e. Integration and of development of interface(s); f. System Testing; g. Training Services; and h. Ad-hoc IM/IT advisory and technical professional services, as and when requested, to support SSC-led activities (e.g. Data clean-up).	sections 5 to 11
e) Transition Services, including: a. Develop Transition plan; b. Conduct knowledge transfer activities; and c. Transfer responsibility for management and operation of ITSM Tool Solution to SSC.	section 12
f) Provision of Application Management Services (AMS), including: a. AMS for a one year following implementation; and	section 13

b. (Optional) AMS for up to nine additional 1-year option periods.

1.2 Authorization of Work

SSC will authorize the Work under the contract, using a phased or gated approach. Prior to completion of a particular stage or phase of the ISTM Tool implementation, the Contractor will collaborate with SSC to develop the requirements to deliver the subsequent stage or phase of the ISTM Tool implementation. As and when request Work, may be delivered on a on a Maximum Price and/or Firm Price basis, and will be authorized using Task Authorizations (TAs) in accordance with Contract Clause 5.7 Task Authorization.

2 CONTRACTOR MANAGEMENT AND OVERSIGHT SERVICE REQUIREMENTS

2.1 Contractor Governance

The Contractor must utilize the governance model contained in the Contractor's Bid to manage its Work. The Contractor governance model must work in conjunction with, and be complementary to SSC's Enterprise ITSM Tool Project governance structure. The Contractor's governance model must identify, at a minimum, individuals to fulfill the following responsibilities:

a) **Customer Executive -** A senior executive resource with overall responsibility, on behalf of the Contractor, for all obligations under this Contract that is the escalation point for issues that cannot be resolved at an operational level. The designated senior executive is the point of contact for the SSC Chief Information Officer (CIO) and the Enterprise ITSM Tool Project Executive Sponsor. This role is to be fulfilled at no direct cost to SSC and the designated individual must be clearly specified in the Contractor Governance Model.

b) **Contractor Project Manager** – A senior project management resource with responsibility, on behalf of the Contractor, for the delivery of the Work. The designated Contractor Project Manager (Contractor PM) is the point of contact for the SSC Project Manager (i.e. Technical Authority) and the primary interface with the ITSM Process Maturity Solution contractor. The Contractor PM must support Enterprise ITSM Tool Project Reporting requirements and other project management meetings as requested. The Contractor PM is responsible for managing the relationship between the Contractor and SSC's Business and IT stakeholders. This role and the designated individual must be clearly specified in the Contractor Governance Model.

c) **ITSM Software Publisher Representative** - If the Contractor is not the Software Publisher, the Contractor must include a representative from the ITSM Tool Software Publisher as a member of the Contractor's Governance Team. The role of the ITSM Tool Software Publisher Representative is to provide general input and guidance to the Contractor's Governance Team, the Contractor's Delivery Team and SSC with respect to the capabilities of the ITSM Tool and the future direction of the COTS software product as well as identify technical experts from the ITSM Tool Software Publisher that may be required to support the implementation of the ITSM Tool Solution. This role is to be fulfilled at no direct cost to SSC and the designated individual must be clearly specified in the Contractor Governance Model.

2.2 Project Management and Oversight

The Contractor must provide Project Management and Oversight services as follows:

a) The Contractor must provide a Project Management Team consisting of:

   a. A Contractor Project Manager (PM), named in the Contractor's Bid, that is dedicated on a full-time basis to provide services under the Contract, on-site at SSC in the National Capital Region (NCR) for a minimum of 24 months. Although the Contractor PM may be involved in the delivery of other as and when requested Work, the Contractor must not double-bill the services of the Contractor PM.

   b. Any additional resources the Contractor deems necessary, in accordance with the Contractor's Bid, dedicated on a full or part-time basis to support the Project Management

and Oversight function as set out in this section.

b) The Contractor Project Management Team is responsible for overseeing the quality of Work delivered by its resources as well as managing its resources to ensure the Work is completed within the budget and schedule set out in the Contract.

c) The Contractor Project Management Team must apply project management discipline in accordance with industry standards as well as align to the SSC Project Governance Framework (PGoF) to ensure that all Work tasks (including deliverables) and activities are fully integrated, such that the performance, time, cost, quality and risk elements associated with the Contractor's Work are fully managed, controlled and scheduled for the duration of the contract.

d) The Contractor Project Management Team is responsible and accountable for delivery of the ITSM Tool Solution and will provide deliverable updates (i.e. Performance Reporting) to the SSC PM utilizing the SSC PGoF standard. (Note: The SSC PM will be responsible for tracking the overall Project progress, including ITSM Tool Solution deliverables)

e) The Contractor Project Management Team must utilize project management monitoring and controlling mechanisms to keep the SSC PM fully aware of the status of the Work at all times.

f) The Contractor Project Management Team must implement, maintain and use the Contractor Work Plan and Schedule (CWP&S) and Contractor Schedule (CS) to maintain management control over all aspects of the Work, throughout the performance period of the Contract to meet cost, schedule and performance objectives and risk reduction goals.

2.3 Contractor's Work Team

a) To deliver the Work, the Contractor must make available and utilize professional services resources to fulfil the job category roles (as applicable) described in section 2.13.

b) The Contractor must establish a Work Team, led by a dedicated Contractor Project Manager (as stipulated in section 2.1).

c) The Contractor's Work Team must:

   a. Provide continuity, consistency and corporate memory through-out the detailed planning and implementation of the Enterprise ITSM Tool Solution;
   b. Provide the Enterprise ITSM Tool software implementation and functional expertise and leadership required to support SSC in its' Enterprise ITSM Tool Project responsibilities; and
   c. Provide adequate professional services resources and expertise to support the delivery of the work in accordance with the Contractor's Work Plan and Schedule as set out in section 2.5.

d) The composition of the Contractor's Work Team, and the level of effort associated with each resource, is at the discretion of the Contractor and may differ during the performance of each specific deliverable and/or TA under the Contract, but at a minimum must include the following:

   a. Resources, named in the Contractor's Bid, to fulfill the following key roles, on-site at SSC in the NCR, on a full-time or part-time basis as determined by the Contractor, during the performance of each Deliverable
      i. Solution / Application Architect, and
      ii. Integration Specialist.
   b. Additional professional services resources and expertise as necessary to support the

performance of each specific deliverable under the Contract.

2.4 Location of Work

a) The Work must be delivered on-site at SSC's location.

b) SSC will provide office accommodations for the Contractor's Work Team on-site at a GC location in the NCR including:
- Workspaces comprised of work surfaces, personal storage unit and chair, sized according to Government of SSC Fit-up Standards;
- Individual computer workstations with SSC approved software, including standardized Project Tools, installed on each Workstation;
- Access to general file storage; and
- Access to networked scanner and printer.

c) All information must remain on SSC-owned hardware and hard copy documents must remain on-site at SSC. Information must be properly safeguarded.

d) If the Contractor has appropriate Facility Clearances, the Application Management Services as set out in SOW section 13, may be delivered remotely from the Contractor's Canadian Operations Centre location upon approval from the SSC Project Manager.

2.5 Contractor Work Plan and Schedule

a) During the delivery of the Contractor Onboarding activities set out in SOW section 5, the Contractor PM must develop a Contractor Work Plan and Schedule (CWP&S) for SSC PM acceptance. The accepted CWP&S will be the baseline for the Contract.

b) The CWP&S must show the overall schedule for completion of the required Work and must clearly identify the tasks, milestones, deliverables, interdependencies and critical path. The CWP&S must align with the defined work objectives and schedule for the Contractor's scope of work defined by the SSC.

c) The Contractor PM must implement, maintain current and use the CWP&S to maintain management control over all aspects of the Work, throughout the performance period of the Contract to meet cost, schedule and performance objectives and risk reduction goals identified in the Contract.

d) Upon approval to proceed with additional as and when requested work, the Contractor PM must update the CWP&S. The updated CWP&S must be provided, in both hard-copy and electronic formats (including native Microsoft Project and .pdf), to the SSC PM within five business days of SSC approval to proceed.

e) The Contractor PM must provide the SSC PM monthly updates on the status of the CWP&S. The format and schedule for progress reporting (including face-to-face meetings between the SSC PM and the Contractor PM) will be determined during the Contractor Onboarding activities set out in SOW section 5.

2.6 Project Reporting and Governance Meetings

a) The Contractor must be prepared to review and discuss the following items with the SSC PM at the

weekly Work Progress Review Meeting:

a. progress to date;
b. latest progress status report;
c. variation from planned progress and the corrective action to be taken during the next reporting period;
d. proposed changes to the schedule;
e. progress on action items, problems or special issues;
f. a general explanation of foreseeable problems, and proposed solutions including an assessment of their impact on the Contract in terms of cost, schedule, technical performance and risk. The proposed solution should include the time and effort involved;
g. any deliverables submitted between progress status review meetings;
h. milestones (technical and financial);
i. schedule and cost performance targets;
j. contract fund status;
k. activities planned for the next reporting period;
l. Project Delivery Management monitoring;
m. Project Performance Indicators;
n. Support Earned Value Reporting (% complete); and
o. Other topics that may be in need of attention.

b) The Contractor must maintain a prioritized Action Item register to record and track the status of:

   a. Action items assigned to the Contractor during the various Enterprise ITSM Tool Project Reporting and Project Governance meetings, and

   b. Interdependencies (i.e. Action Items for which the Contractor is awaiting feedback/action from SSC).

c) The Contractor must assure and provide evidence that decisions as a result of the various Enterprise ITSM Tool Project Reporting and Project Governance meetings are implemented as applicable.

d) In addition to the formal Enterprise ITSM Tool Project Reporting and Project Governance meetings, SSC, at its sole discretion, may call upon the Contractor to provide representation at special meetings. Special meetings are intended to address matters of a serious nature that cannot reasonably be delayed until the next scheduled formal progress status review meetings.

e) SSC reserves the right to adjust the frequency and composition of the Enterprise ITSM Tool Project Reporting and Project Governance meetings as required during the contract period.

2.7 Monthly Progress Report

The Contractor must prepare and deliver a Monthly Progress Report which describes the status of the activities, deliverables and timetable, which are used to update the CWP&S. This report must be submitted to the SSC PM within ten business days following the end of each month. The Progress Review and Contract Status meeting will be held following receipt of this report. The Contractor will determine the format and content of the Monthly Progress Report, but at a minimum it must provide the information contained in

the following sample Table of Contents:

1. Executive Summary

2. Project Current Phase Information
2.1. Software Development Lifecycle (SDLC) Phase
2.2. % Completed
2.3. Plan Start
2.4. Plan Complete
2.5. Actual Start

3. Progress Report Summary
3.1. Key Project Deliverable
3.2. Status
3.3. Planned Completion Date
3.4. Revised Completion Date
3.5. Actual Completion Date

4. Accomplishments This Period

5. Plans for Next Period

6. Issues and Problems Requiring Attention or Action
6.1. Project Issues
6.1.1. Description including affected area
6.1.2. Proposed Resolution
6.1.3. Planned Resolution Date
6.1.4. Action taken
6.1.5. Revised Resolution Date
6.1.6. Actual Resolution Date

2.8 Quality Management Plan

a) The Contractor must use a formal Quality Management (QM) Plan to ensure that all deliverables to SSC are of high quality[1]. The QM plan must include internal quality assurance processes to ensure the overall quality and functionality of the outputs delivered under the Contract. The QM plan must include processes for performance of reviews, inspections and tests necessary to substantiate that the services and material provided conform to the specifications and requirements of the Contract. The QM plan must also ensure that Contractor's resources provided under the Contract are knowledgeable and experienced in the use of the Contractor's QM program and processes. SSC will conduct user acceptance testing (UAT) of the new applications and any deficiencies must be rectified by the Contractor within the agreed upon timeline.

b) The QM Plan will be delivered as part of Contractor Onboarding as set out in section 5 of this SOW.

[1] Quality is defined as the degree to which the deliverable fulfills the stipulated requirements to SSC standards as determined during Contractor Onboarding.

The Contractor will determine the format of the QM Plan, but at a minimum it must provide the information noted in a) above and the following sample Table of Contents:

1. Introduction – an overview of the QM document
2. Purpose – what is the purpose for the QM Plan
3. Scope – what is the scope of the QM Plan
4. Definitions and acronyms – definitions of all terms
5. References – documents used to prepare the QM Plan
6. Quality Management processes – description of the QM processes to be used by the contractor
7. Quality Roles and responsibilities
8. Quality checkpoints / deliverable reviews
9. Standards, practices and guidelines
10. Metrics

c) The Contractor must obtain SSC PM acceptance of the QM Plan. SSC, at its discretion, may not authorize the Contractor to proceed with Work until the SSC PM has approved the QM Plan.

d) The Contractor must manage the quality of their Work in accordance with the accepted QM Plan.

e) The Contractor must, as and when requested, update the accepted QM Plan to reflect lessons learned following Release 1 and/or subsequent Releases of the ITSM Tool Solution.

2.9 Risk Management

a) The Contractor must develop and maintain a Risk Management Plan for the Work to be delivered under the Contract. The Risk Management Plan will be delivered as part of Contractor Onboarding as set out in section 5 of this SOW. The Contractor will determine the format and content, but at a minimum it must provide the information contained in the following sample Table of Contents:

1. Introduction – an overview of the document
2. Purpose – what is the purpose for the risk management plan
3. Scope – what is the scope of the risk management plan
4. Definitions and acronyms – definitions of all terms
5. References – documents used to prepare the risk management plan
6. Risk Summary – the overall amount of risk in the project
7. Risk Identification – A list of key risks identified by the contractor that may impact the deliverables under the contract and description of these risks
8. Risk Management Process/Tasks – a description of the tasks to be performed to manage risks during the project. The plan must include:
   8.1. The approach used to identify the risks
   8.2. How the risks were analyzed and prioritized
   8.3. Strategies used such as mitigation, avoidance, prevention and others
   8.4. Tools and Techniques that will be used to control and monitor risk
   8.5. How the status will be monitored, risk reviewed and reporting schedules
9. Organization and Responsibilities – The list of individuals involved with the managing of risk and their roles and responsibilities

b) The Contractor must maintain a Contract Risk and Issues Log. Unless otherwise agreed to by the SSC PM, the Contractor must submit the Contract Risk and Issues Log to SSC for integration with the Enterprise ITSM Tool Project Risk Register.

c) The Contractor must conduct regular bi-weekly meetings (or more frequently if determined by the

Contractor PM) to review the risks and issues log and must produce formal minutes of these meetings. The SSC PM must have access to these minutes. The Contractor will invite the SSC PM to participate in these meetings as appropriate.

d) The Contractor PM must obtain SSC PM acceptance of the Risk Management Plan.

e) The Contractor must manage the Work in accordance with the accepted Risk Management Plan.

f) The Contractor must, as and when requested, update the accepted Risk Management Plan to reflect lessons learned following Release 1 and/or subsequent Releases of the ITSM Tool Solution.

2.10 Deliverable Review and Acceptance Process

a) The Contractor must develop and document, in collaboration with SSC, a Deliverable Review and Acceptance Process that will be used to submit applicable Contractor deliverables for SSC PM acceptance. The Deliverable Review and Acceptance Process will be delivered as part of Contractor Onboarding as set out in section 5 of this SOW.

b) The document must identify the various categories (i.e. types) of deliverables that will be provided under the Contract; identify which categories are subject to the formal Deliverable Review and Acceptance Process; establish the process, responsibilities and timelines (by deliverable category) for each step in the process (including review, corrective action and acceptance); and establish the mechanism for formal SSC PM acceptance.

c) The Contractor PM must obtain SSC PM acceptance of the Deliverable Review and Acceptance Process.

d) The Contractor must manage the Contract in accordance with the accepted Deliverable Review and Acceptance Process.

e) The Contractor must, as and when requested, update the accepted Deliverable Review and Acceptance Process to reflect lessons learned following Release 1 and/or subsequent Releases of the ITSM Tool Solution.

2.11 Format and Language of Deliverables

a) Unless otherwise specified in the contract, one hard copy and one electronic copy of each deliverable must be provided to the SSC PM. Deliverables must be provided in MS Office Suite format, using the then current version in use at SSC (**Note:** SSC is currently upgrading to MS Office version 2013).

b) All deliverables must be provided in English. SSC reserves the right to translate applicable deliverables to French.

c) The Contractor must maintain on SSC's premises an electronic library of all Work in progress, delivered items and review comments, and must perform version control.

2.12 Professional Services Resources

The Contractor must provide qualified Professional Service (PS) resources in the resource categories identified below as required to meet the requirements of the Contract.

1) Contractor Project Manager
2) Project Coordinator
3) Business Analyst
4) Solution/Application Architect
5) Integration Specialist
6) Information Architect
7) Infrastructure / Technology Architect
8) Programmer/Software Developer
9) User Experience (UX) Specialist
10) Test Manager
11) Tester
12) Courseware Developer
13) Instructor
14) Data Entry Clerk
15) Data Conversion Specialist
16) Database Modeller / IM Modeller
17) Database Administrator
18) System Analyst
19) Operations Support Specialist
20) Change Management Consultant

Additional PS resources categories may be added, as agreed between SSC and the Contractor, if required to support the delivery of Work described herein.

NOTE: SSC reserves the right to request that the Contractor demonstrate the qualification (i.e. knowledge and experience) of any resource proposed in response to a Task Authorization. Senior resources must have > 10 years of experience associated with the role; Intermediate resources must have 5-10 years of experience, and Junior resources < 5 years.

2.12.1 Contractor Project Manager (Contractor PM)

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Conduct project management activities and produce project management artifacts and deliverables as per the agreed to methodology;
b) Manage the Work to be delivered under the Contract by ensuring that resources are made available and that the Work is developed and is fully operational within previously agreed time, cost and performance parameters;
c) Determine the composition, roles and responsibilities, budgetary requirements and terms of reference for the Work to be delivered under the Contract;
d) Develop and maintain project Work Breakdown Structures and schedules, conducting critical path analysis and identifying project scheduling and dependency issues for the Work to be delivered under the Contract;
e) Lead agile development practices including but not limited to Release Planning and SPRINT

planning;
f) Coordinate integration/customization activities involving data integration and/or common components with SSC SMEs;
g) Coordinate infrastructure setup activities with SSC SMEs;
h) Procure and provide third party products as required under the Contract; and
i) Report progress of the Work to be delivered under the Contract on an ongoing basis and at scheduled points in the life cycle.

2.12.2 Project Coordinator

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Assist the Contractor PM in developing and maintaining/updating the Contractor's project control and reporting documents;
b) Liaison, on behalf of the Contractor PM, with technical and business project team members to obtain status updates;
c) Assist Contractor Work Team members in performing administrative tasks to support project tasks and activities;
d) Use MS Office (including Word, PowerPoint, Excel, and Visio) to perform work;
e) Use MS Project to update the Contractor's project schedule;
f) Use document management software to perform work;
g) Maintain Contract documents and track the Contractor's change requests;
h) Coordinate project team meetings and events and prepare minutes/notes; and
i) Support the Contractor PM with other project responsibilities as requested.

2.12.3 Business Analyst

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Participate in project management activities (e.g. SCRUMs) and perform as SCRUM Master when requested by Contractor PM;
b) Lead requirements gathering and refinement and development of detailed requirements;
c) Work with business sponsors very early in system development to define ITSM end-user roles and permission sets for system;
d) Facilitate and co-lead business functionality prototyping sessions with ITSM Tool specialists (especially customer-facing sessions);
e) Establish acceptance test criteria with customer;
f) Participate in definition of ITSM Tool related UAT and PROD sanity tests;
g) Ensure traceability of requirements to sprint "releases";
h) Organize SSC facing meetings and coordinate communications with SSC regarding development and test tasks;
i) Perform business analyses of functional requirements to identify information, procedure, and decision flows;
j) Evaluate existing procedures and methods, identify and document items such as database content, structure, application subsystems;
k) Develop data dictionary;
l) Define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems; and
m) Identify candidate business processes for re-design, prototype potential solutions, provide

trade-off information and suggest a recommended course of action.

2.12.4 Solution / Application Architect

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Identify the policies and requirements that drive out a particular solution architecture;
b) Develop solution architectures, frameworks and strategies to meet the business and nonfunctional requirements;
c) Provide expert guidance and advice regarding the Enterprise ITSM Tool features & administration in support of the definition and implementation of business solutions;
d) Work with architecture governance bodies to review work products ensuring standards are met;
e) Select an architectural approach that is consistent with the customer's architectural standards and development practices that maximizes use of the customer's existing technology standards;
f) Analyze and evaluate alternative business solutions to meet business problems, propose and seek approval for use of new technologies when existing technology standards do not support requirements ;
g) Ensure the effective integration of all aspects of the business solutions;
h) Ensure the business solution meets functional and nonfunctional security requirements;
i) Conduct workshops with stakeholders to ensure alignment and consensus, on the solution architecture;
j) Monitor industry trends and Government of SSC policies and directives to ensure that business solutions fit with government and industry directions for ITSM technology;
k) Monitor applicable software vendor roadmaps and plans to ensure that the proposed solution architecture is robust to vendor driven change;
l) Provide leadership and guidance to technical leads and subject matter experts;
m) Analyze functional and nonfunctional requirements to identify information procedures and data flows within the business solution;
n) Define application tiers. frameworks, component types and interfaces, as necessary to design, communicate and develop a business solution;
o) Evaluate existing procedures and methods, identify/document existing structured and unstructured information repository interfaces/content, identify/document existing application interfaces/sub-systems, identify/document existing integration between architectural components;
p) Define and document interfaces of manual to automated operations within application sub-systems, to external systems and between new and existing systems;
q) Provide advice and guidance to developers and other stakeholders who are responsible for implementing the business solution; and
r) Identify and document system specific standards relating to programming, documentation and testing, program libraries, data dictionaries, naming conventions etc.

2.12.5 Integration Specialist

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Develop data integration objects and data processing flow using current tools and software;
b) Act as the technical lead for initiatives that involve data translation or integration

development;
c) Resolve highly complex technical data communication and transformation issues;
d) Design, test and implement data translation objects (maps);
e) Troubleshoot technical issues related to data transformation and flow;
f) Analyze customer system and data specifications and provide gap analysis; and
g) Create documentation for future reference, training and support purposes.

2.12.6 Information Architect

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Lead or perform information/data modeling in support of business process re-engineering (BPR) activities and in support of business requirements and nonfunctional requirements;
b) Provide technical assistance, guidance and direction in terms of structured and unstructured data analysis and modeling to team members;
c) Lead or participate in the development of data modeling, data quality and metadata policies and procedures;
d) Lead or provide advice in developing and integrating information models between business processes to eliminate information redundancies and assure data integrity;
e) Lead or provide advice in developing master data management aspects of the resulting System;
f) Work with the Solution Architect to ensure effective data integration within the resulting System;
g) Lead the strategy, plan and design required for data migration and reconciliation processes;
h) Produce source-target mapping specifications for use by the BI Developer for data integration and data migration processes;
i) Lead or provide advice regarding data considerations for analytics and reports;
j) Participate in data analysis as a result of new/updated requirements;
k) Comply with corporate data architecture standards, strategies and frameworks, including enterprise data warehouse activities;
l) Provide input to refinement of legacy data architectures, as necessary to meet business and nonfunctional requirements;
m) Analyze and evaluate alternative information architecture solutions to meet business problems/requirements and incorporate into SSC architecture;
n) Work closely with business stakeholders and information governance bodies to develop or align to information standards;
o) Work with the Solution Architect to ensure the solution meets functional and nonfunctional data security requirements; and
p) Review organization and GC architecture strategies and directions, data requirements, and business information needs and devise data structures to support them.

2.12.7 Infrastructure / Technology Architect

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Lead or participate in definition and development of technical infrastructure architectures, farm topologies and strategies to meet the business and nonfunctional requirements;
b) Provide expert guidance and advice regarding the setup, administration, configuration and integration of the Enterprise ITSM Tool in support of business solutions;
c) Lead or participate in developing scripts to automate setup of environmental infrastructure

per technical architecture specifications;
d) Work with architecture governance bodies (e.g. SSC Senior Architecture Review Board SARB) to review work products that ensure standards are met;
e) Identify the policies and requirements that drive out a particular solution;
f) Lead or participate in analyzing and evaluating alternative technology solutions, including Commercial Off the shelf (COTS) and Open Source products that are consistent with the customer's architectural standards, to support the business solution;
g) Obtain approval for use of new technologies when existing technology standards do not support the business and nonfunctional requirements;
h) Ensure the integration of all aspects of technology solutions;
i) Ensure technology solutions are in compliance with security policies and requirements;
j) Participate in and assess results from Fit Gap assessments of various technology options;
k) Monitor industry trends to ensure that technical architectures fit with government and industry directions for technology;
l) Monitor vendor roadmaps and plans to ensure that the proposed technical architecture is robust to vendor driven change;
m) Provide information, direction and support for emerging technologies;
n) Lead or participate in impact analysis of technology changes;
o) Provide support to applications and technical support teams in the proper application of existing infrastructure;
p) Lead or participate in the review of the technical infrastructure design to recommend performance improvements;
q) Evaluate hardware and software relative to their ability to support specified requirements and, by determining potential and actual bottlenecks, and improve system performance through recommended hardware changes; and
r) Review computer software systems and data requirements as well as communication and response needs to plan for network and storage capacity.

2.12.8 Programmer/Software Developer

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Develop and prepare diagrammatic plans for solution of business, scientific and technical problems by means of computer systems of significant size and complexity;
b) Configure the Enterprise ITSM Tool COTS software and other selected components to map to the business processes and functional requirements as defined in the systems designs;
c) Analyze the problems outlined by systems analysts/designers in terms of such factors as style and extent of information to be transferred to and from storage units, variety of items to be processed, extent of sorting, and format of final printed results;
d) Select and incorporate available software programs;
e) Design detailed programs, flow charts, and diagrams indicating mathematical computation and sequence of machine operations necessary to copy and process data and print the results;
f) Translate detailed flow charts into coded machine instructions and confer with technical personnel in planning programs;
g) Verify accuracy and completeness of programs by preparing sample data, and testing them by means of system acceptance test runs made by operating personnel;
h) Correct program errors by revising instructions or altering the sequence of operations; and
i) Test instructions, assemble specifications, flow charts, diagrams, layouts, programming and

operating instructions to document applications for later modification or reference.

2.12.9 User Experience (UX) Specialist

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Design and conduct user research using methods such as: ethnographic field studies, participatory design sessions, site visits, focus groups, benchmark studies, usability studies, heuristic evaluations, and similar approaches;
b) Synthesize findings to inform a better understanding of end users, give insight into business value, and identify potential usability issues and design opportunities;
c) Identify potential usability issues and design opportunities;
d) Convert research findings into actionable results;
e) Design prototypes, screen mockups, and wireframes based on the results of usability testing and customer feedback;
f) Communicate analysis, recommendations, and potential design solutions verbally and through documentation to the project team and key stakeholders;
g) Work collaboratively with other team members to define and improve the user experience;
h) Advocate for the end user by influencing decisions to ensure that product and design decisions are aligned with user needs and expectations;
i) Organize and lead lab-based user testing, remote testing, paper prototype testing, iterative prototype testing, and concept testing;
j) Ensure solutions are accessible and intuitive; and
k) Make enhancement recommendations as needed.

2.12.10 Test Manger

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Develop test strategies and plans where multiple development teams are situated in different geographic locations, working with Testers, Developers and Architects as necessary;
b) Drive resolution of defects;
c) Provide advice, guidance and coordination efforts for execution of test strategies and plans where multiple development teams are situated in different geographic locations;
d) Provide advice, guidance and coordination efforts for selection of automated testing tools that are consistent with customer technology standards and the business solution;
e) Plan, organize, and schedule testing efforts for large systems, including the execution of systems integration tests, performance and stress tests and user acceptance testing (e.g., stress tests);
f) Supervise testing in accordance with the test plan;
g) Manage and monitor test plans for all levels of testing;
h) Manage walkthroughs and reviews related to testing and implementation readiness; and
i) Present results of tests relative to acceptance criteria to various stakeholders including

business customers.

2.12.11 Tester

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Participate in Test planning and coordination;
b) Prepare and provide status reports to a Test Manager or the Contractor PM;
c) Develop test scenarios and test scripts;
d) Establish and maintain source and object code libraries for a multi-platform, multi-operating system environment;
e) Establish software testing procedures for unit test, integration testing and regression testing with emphasis on automating the testing procedures;
f) Establish and operate "interoperability" testing procedures to ensure that the interaction and co-existence of various software elements, which are proposed to be distributed on the common infrastructure, conform to appropriate departmental standards (e.g. For performance, compatibility, etc.) and have no unforeseen detrimental effects on the shared infrastructure; and
g) Establish a validation and verification capability which assumes functional and performance compliance.

2.12.12 Courseware Developer

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Perform needs assessment/analysis for training purposes;
b) Plan and monitor training projects;
c) Perform job, task, and/or content analysis;
d) Write criterion-referenced, performance-based objectives;
e) Recommend instructional media and strategies;
f) Develop performance measurement standards;
g) Develop training materials;
h) Prepare end-users for implementation of courseware materials; and
i) Communicate effectively by visual, oral, and written form with individuals, small groups, and in front of large audiences.

2.12.13 Instructor

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Assess the relevant characteristics of a target audience;
b) Prepare end-users for implementation of courseware materials;
c) Conduct training courses; and
d) Communicate effectively by visual, oral, and written form with individuals, small groups, and

in front of large audiences.

2.12.14 Data Entry Clerk

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Enter data from various sources and formats into a computer program according to a pre-described format;
b) Searching for the required information to be entered form a repository of unstructured data (Microsoft Office documents, PDF documents), extracting the relevant data (cutting) and copying (pasting) to structured data fields in the computer program;
c) Verifying the data entered for errors and correcting as required;
d) Use MS Office (including Word, PowerPoint and Excel) to perform work; and
e) Use document management software to perform work.

2.12.15 Data Conversion Specialist

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Oversee all facilities of the conversion process;
b) Complete mapping, interfaces, mock conversion work, enhancements, actual conversion, and verify completeness and accuracy of converted data;
c) Establish a strong working relationship with all customers, interact effectively with all levels of customer personnel, and provide conversion support;
d) Analyze and coordinate data file conversions; and
e) Work with importing files from heterogeneous platforms.

2.12.16 Database Modeller / IM Modeller

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Design, develop and maintain Logical Data Models;
b) Analyze proposed changes to databases from the context of the Logical Data Model;
c) Provide technical expertise in the use and optimization of data modeling techniques to team members;
d) Provide technical assistance, guidance and direction in terms of data analysis and modeling to team members;
e) Provide assistance to project team and business users relating to data issues and data analysis concepts;
f) Participate in the development of data modeling and metadata policies and procedures;
g) Participate in data analysis as a result of new/updated requirements;
h) Apply approved changes to logical data models;
i) Comply with corporate data architectures, strategies and frameworks, including enterprise data warehouse activities;
j) Analyze and evaluate alternative data architecture solutions to meet business problems/requirements to be incorporated into the corporate data architecture;
k) Review corporate architecture strategies and directions, data requirements, and business information needs and devise data structures to support them;
l) Improve modeling efficiency through recommendations on how to better utilize current

metadata repositories;
m) Comply with corporate repository metadata directions;
n) Provide input to refinement of data architectures;
o) Participate in data architecture refinement;
p) Define access strategies; and
q) Construct, monitor and report on work plans and schedules.

2.12.17 Database Administrator

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Customize database conversion routines;
b) Finalize Conversion Strategy;
c) Generate new database with the customer;
d) Maintain data dictionaries;
e) Develop and implement procedures that will ensure the accuracy, completeness, and timeliness of data stored in the database;
f) Develop and implement security procedures for the database, including access and user account management;
g) Advise programmers, analysts, and users about the efficient use of data;
h) Maintain configuration control of the database;
i) Perform and/or coordinate updates to the database design;
j) Control and coordinate changes to the database, including the deletion of records, changes to the existing records, and additions to the database;
k) Ensure backup and disaster recovery procedures are in place; and
l) Develop and implement data conversion procedures which extract, transform and load data from source systems to a data warehouse.

2.12.18 System Analyst

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Implement applications to support projects, departments, organizations or corporate services;
b) Translate business requirements into systems design and technical specifications;
c) Analyze and recommend alternatives and options for technical solutions;
d) Analyze business requirements, perform feasibility studies, provide costing estimates for options analysis, map interdependencies, and produce the required functional and technical specifications or process re-engineering recommendations;
e) Provide system expertise to both functional and technical teams to ensure effective integration of solutions across the application(s); and
f) Provide application support to end-users by troubleshooting and correcting issues, providing training, and reporting to management.

2.12.19 Operations Support Specialist

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Provide systems administration and systems operations support, including setting up user

access, user profiles, backup and recovery, day-to-day computer systems operations;
b) Perform software upgrades, and apply patches;
c) Provide customer interface to ensure requested changes are implemented;
d) Monitor computer workload trends and make adjustments to ensure optimum utilization of computer resources; and
e) Provide expertise in the areas of IT Infrastructure, Servers and Operating Systems to development teams.

2.12.20 Change Management Consultant

Typical tasks and activities associated with role include, but are not limited to, the following:

a) Work with the client team to conduct organizational change management (OCM) activities;
b) Assist client to assess the overall organization and the organizational units affected by the change and its capacity/capability to undertake and successfully deliver a project;
c) Support client in defining the change management and communication strategies;
d) Assist the client in planning the change management implementation and implementing the change;
e) Interact with the client project team members to implement changes to the organization;
f) Assess the client project team's dynamics and conduct regular project team building sessions;
g) Monitor and evaluate the client's performance once the change has been implemented;
h) Meet in conference with stakeholders and other project managers and recommending an action plan to move forward with a change management program;
i) Develop internal OCM communication plans related to the project implementation including the identification of communication objectives; target audiences; messages; impediments/ barriers; communication methods; cost analysis and providing recommendations to client Management;
j) Review and provide recommendations and input to OCM communication and information products;
k) Support the client in the development of plans, presentations, tables, diagrams and working with a variety of project management tools in support of the change management program; and
l) Support the client project team to deliver presentations to stakeholders and end users to launch and support the OCM program.

3 ITSM TOOL SOFTWARE REQUIREMENTS

3.1 Contractor Requirements

a) The Contractor must provide an ITSM Tool (i.e. perpetually licensed COTS software), as identified in the Contractor's Bid.

b) The Contractor must provide ISTM Tool licenses to support three classes of users as follows:

User Class	Definition
ITSM Tool User	a) Entitled to use all functionality provided by the ITSM Tool including the requirements set-out in Appendix 2 – ITSM Tool Functional Requirements to support the roles (as assigned by the System Administrator) associated with the Service Management processes listed below: a. Service Asset Configuration Management b. Incident Management c. Request Fulfillment d. Change Management e. Service Catalogue Management f. Service Level Management g. Event Management h. Knowledge Management i. Problem Management j. Release and Deployment Management k. Demand Management l. Capacity Management m. IT Financial Management n. Availability Management b) Also a Service Consumer as defined below.
ITSM Tool Configuration & Development	Entitled to configure the ITSM Tool using all configuration settings and methods included with the product for the purpose of ITSM Tool system administration and service management process configuration, and to develop customizations to the software.
Service Consumer	Entitled to use all functionality provided by the ITSM Tool's self-service portal, accessed via any channel (e.g. web browser, mobile, etc.), including the requirements set-out in section 2, Self-Service Portal (SSP) of Appendix 2 – ITSM Tool Functional Requirements.

c) The ITSM Tool must be from a single Software Publisher with a single user interface and common look and feel.

d) The ITSM Tool must not be limited to a specific infrastructure environment and can be transferred, in whole or in part, from one environment to another as SSC, at its sole discretion, sees fit.

e) The current commercially available version of the ITSM Tool provided by the Contractor must meet each of the Non-Functional Requirements set out in Appendix 1 to this SOW.

f) The current commercially available version of the ITSM Tool provided by the Contractor must meet the Functional Requirements, set out in Appendix 2 to this SOW, by leveraging configuration settings that are available in the software, and where configuration of the ITSM Tool, the resulting feature, business rule or workflow is limited to the following actions:

    a. Must be configured using screens or files that are documented in the software manufacturer's manuals. This may include:
        i. Filling out a form in an administration GUI in the ITSM Tool.
        ii. Clicking a button or a link
        iii. Changing a documented setting in a configuration file
        iv. Running a wizard

    b. Must not require coding or knowledge of any industry or proprietary coding or scripting language.

    c. Must not involve modifications or overlays of objects or components originally shipped with the product.

    d. Must be supported by the Software Publisher's standard Maintenance and Support Services for the Licensed Software.

    e. Must be recognised by the Software Publisher's commercially available upgrade installers. In other words, the configuration must not require any additional backup, reconciliation, regression testing or analysis when upgrading the ITSM software, than functionality originally shipped with the product.

g) The Contractor must provide documentation for the ITSM Tool, in both English (Canadian) and French (Canadian that includes at a minimum the following:

    a. Installation Guide

    b. Administration Guide

    c. User Guide

    d. Release Notes

    e. Performance Tuning and capacity planning guidance.

h) The Contractor must provide Software Maintenance and Support for the ITSM Tool, that includes at a minimum the following:

Software Maintenance and Support Service	Requirements
a) Software Error Correction Services	1. Canada may report to the Contractor any failure of the Licensed Programs to operate in accordance with the Software Documentation or, if applicable, the Specifications during the Software Support Period. Canada may report failures either in writing or by telephone or other remote communication. Upon receipt of a report of a failure from Canada, unless provided otherwise in the Contract, the Contractor must use all reasonable efforts to provide Canada within the time frames established in subsections 2 and 3, with a correction of the Software Error which caused the failure. Any such software correction must cause the Licensed Programs to meet the Software Documentation or, if applicable, the Specifications during the Software Support Period. The Contractor must use all reasonable efforts to provide permanent corrections for all Software Errors and the Contractor warrants that the Licensed Software will meet the functional and performance criteria set out in the Specifications. All Software Error corrections will become part of the Licensed Software and will be subject to the conditions of Canada's license with respect to the Licensed Software. 2. Unless provided otherwise in the Contract, the Contractor must respond to a report of a Software Error in accordance with the severity of the Software Error, as detailed in subsection 3. The severity will be reasonably determined by Canada, and communicated to the Contractor, based on the following definitions: • "Severity 1": indicates total inability to use a Licensed Program, resulting in a critical impact on user objectives; • "Severity 2": indicates ability to use a Licensed Program but user operation is severely restricted; • "Severity 3": indicates ability to use a Licensed Program with limited functions which are not critical to overall user operations; • "Severity 4": indicates that the problem has been by-passed or temporarily corrected and is not affecting user operations.

Software Maintenance and Support Service	Requirements
	3. Unless provided otherwise in the Contract, the Contractor must use reasonable efforts to correct Software Errors as follows: • "Severity 1": within twenty-four (24) hours of notification by Canada; • "Severity 2": within seventy-two (72) hours of notification by Canada; • "Severity 3": within fourteen (14) days of notification by Canada; • "Severity 4": within ninety (90) days of notification by Canada. 4. If Canada reports a Software Error to the Contractor, Canada must give the Contractor reasonable access to the computer system on which the Licensed Program resides, and must provide such information as the Contractor may reasonably request, including sample output and other diagnostic information, in order to permit the Contractor to expeditiously correct the Software Error.
b) Maintenance Releases and Upgrades	During the Software Support Period, the Contractor must provide to Canada: 1. All Maintenance Releases, in object-code form, at no additional cost. All Maintenance Releases will become part of the Licensed Software and will be subject to the conditions of Canada's license with respect to the Licensed Software. Unless provided otherwise in the Contract, Canada will receive at least one Maintenance Release during any twelve (12) month maintenance period. 2. Software upgrades for major releases, up to version n-1, of the ITSM Tool.
c) Media	3. The Contractor must provide to Canada all Software Error corrections, Maintenance Releases and updates on Media that are free of defects and of computer viruses, and which are compatible with the computer systems on which the Licensed Programs are installed. 4. Canada will own the Media provided to Canada in the performance of the software support services upon delivery to and acceptance of the Media by or on behalf of Canada. For the purposes of this subsection, "Media"

Software Maintenance and Support Service	Requirements
	does not include the Licensed Software stored on the Media.
d) Support Services	If the Contract provides for support services, the Contractor must provide to Canada access to the Contractor's personnel, to help Canada in answering questions with respect to the Licensed Software, during the hours specified in the Contract. If the hours are not specified in the Contract, this access to the Contractor's personnel must be between the hours of 8:00 a.m. to 5:00 p.m., local time, at the site where the Licensed Programs are installed, Monday through Friday, exclusive of statutory holidays observed by Canada at such site. Canada's access to the Contractor's personnel must include telephone, fax, e-mail and Internet access and, if expressly provided in the Contract, on-site and Swift Action Tactical (SWAT) services. If applicable and if specified in the Contract, Canada will, by notice in writing to the Contractor, appoint a user representative or representatives who will be the only individual(s) entitled to access the support services on behalf of Canada. Canada may change any such appointment by subsequent notice to the Contractor.
e) On-site Services	Unless provided otherwise in the Contract, the monthly or yearly support charge specified in the Contract is inclusive of all software support services described in the Contract, except for On-site services and On-site SWAT response services for Software Error correction. The Contractor must provide on-site services, when requested by Canada, at the hourly or daily labour rates specified in the Contract. Reasonable travel and living costs incurred by the Contractor in connection with on-site services, if approved in advance by Canada, will be reimbursed to the Contractor in accordance with the guidelines specified in the Contract, or, if no guidelines are specified, in accordance with applicable Treasury Board guidelines. All such pre-approved costs must be invoiced to Canada as a separate charge.

i) The Contractor must install the ITSM Tool on all SSC's multi-tenant instances including the Development; Testing; Production; Training; Reporting; and Disaster Recovery environments provided by SSC.

j) **Optional.** If, during the term of the contract, the Contractor makes the ITSM Tool commercially available as a Software as a Service (SaaS) offering, the Contractor must, if requested, make the SaaS solution available to SSC, to provide to its' Clients, on prices and on such additional terms as may be appropriate as agreed by the parties (including but not limited to the requirement to provide credit for existing licenses purchased and transferred to a SaaS model and/or the migration of departmental workloads into a SaaS service at no extra cost). If requested, the terms of the SaaS offering will be negotiated in accordance with the process set out in Annex I – SaaS Negotiation Process and would be considered only if and when all are resolved, and if the two parties are able to reach agreement.

In the circumstances where the Contract agrees to provide the ITSM Tool as SaaS, the ITSM Tool must be hosted on the Contractor or a Subcontractor infrastructure, that is secure, working, complete, bug free, and entirely situated and hosted in Canada on Contractor or Subcontractor data centers, with Canada's data isolated within Canada and the underlying service providing all required infrastructure, network, database, web, application servers, operating systems, virtual machines, and storage to permit the ITSM tool to function as required by the Contract.

The optional requirement for a SaaS solution does not imply that all GC clients which have implemented the ITSM Tool licensed software on premise will migrate to a SaaS offering.

4 INFRASTRUCTURE CAPACITY SPECIFICATION REQUIREMENTS

4.1 Contractor Requirements

a) The Contractor must meet with SSC as required to confirm the capacity requirements specified in the Contractor's Bid for the infrastructure capacity for the Development and Testing environments (to be provided by SSC) to support the estimated minimum number of Users and Volumetric Data for SSC and the first Tenant department, as well as to provide best practice guidance regarding set-up or configuration of the Development and Testing environments.

b) The Contractor must, as part of Contractor Onboarding (set out in section 5), provide specifications for the capacity requirements, as well as best practice guidance regarding set-up or configuration, for the infrastructure to be provided by SSC for the Training environment.

c) The Contractor must, as and when requested, provide specifications for the capacity requirements, as well as best practice guidance regarding set-up or configuration, for the infrastructure to be provided by SSC including, but not limited to, the following environments:

    a. Production environment;

    b. Reporting environment; and

    c. Disaster Recovery environment.

d) The scope of infrastructure capacity specifications must include:

    a. all required hardware (including CPU, memory and storage) and middleware to make the system work including switching to a disaster recovery site with data current to one day; and

    b. hardware for storage for attachments and system log files, etc.

e) The Contractor must, as and when requested, provide the specifications for additional infrastructure required to increase / scale the capacity of the hardware infrastructure as necessary to support additional customers including:

    a. Onboarding of the customer as tenant on SSC's multi-tenant instance; and/or

    b. Onboarding of the customer to a separate instance of the Solution.

f) The Contractor must assume a minimum of 14-weeks lead time for SSC to procure and install any required infrastructure.

5 CONTRACTOR ONBOARDING REQUIREMENTS

5.1 Contractor Onboarding Requirements

The Contractor Onboarding activities will focus on the initiation of services under the Contract as required to establish the detailed plans and SSC-provided infrastructure necessary to commence the Work associated with the Functional Design and Configuration of the ITSM Tool. The Contractor Onboarding activities **must be completed within 90 calendar days of Contract Award**.

The Contractor Onboarding activities must be completed in accordance with the Detailed Work Plan for Contractor Onboarding contained in the Contractor's Bid and must include, at a minimum, the following deliverables:

5.1.1 Deliverable #1: Review and provide feedback to SSC ITSM Process Maturity Solution draft documents

a) Within 10 business days of Contract Award, SSC will provide the Contractor with Enterprise ITSM Tool Project plans and ITSM Process Maturity Solution contactor deliverables. The Contractor must review these documents before the Contractor Solution Impact Meeting (item b that follows). These include, but are not limited to, the following documents:
   i. SSC's Project Governance Framework (PGoF)
   ii. Functional Requirements
   iii. OCM Strategy and Plan
   iv. Latest version of the ITSM Process Maturity Backlog (including User Stories)
   v. Relevant Process Maturity Solutions Contract deliverables, such as:
      a. SSC Operational and Business Needs Document
      b. Process Maturity Implementation Plan
      c. Process Maturity Activity Plan
      d. OCM Strategy and Plan
      e. CMDB Data model and design document
      f. Service Catalogue Design document
      g. Concept of Operations for in scope ITSM processes
      h. Process design documentation for in scope ITSM processes
      i. Process readiness assessment for in scope processes
      j. Process work packages
      k. Integrated Deployment Plan and Checklist
      l. Process Maturity Training Strategy and Plan
      m. Process Improvement and Benefits Realization Strategy

b) Within 15 business days of receipt of documents (above) for review, the Contractor must participate in a Contractor Solution Impact Meeting with the SSC PM and key members of the Project Team. During the meeting the Contractor must:

   i. Identify any information contained in the Enterprise ITSM Tool Project plans and ITSM Process Maturity Solution contactor deliverables documents provided by SSC (listed in a. above), and subsequent clarification from the SSC Project Team, which changes or impacts the requirements set out in this SOW;

   ii. Identify risk and issues arising from these changes or impacts; and

iii. If applicable, review recommended adjustments, to the Contractor's proposed approach or plan set out in the Contractor's Bid, as a result of the a Enterprise ITSM Tool Project plans and ITSM Process Maturity Solution contactor deliverables documents provided by SSC.

5.1.2 Deliverable #2: Rules of Engagement, Governance Model and Core Delivery Team

The Contractor must collaborate with the SSC Enterprise ITSM Tool Implementation Project Team to develop and document the Rules of Engagement between SSC's Project Team and the Contractor and onboard the initial Contractor resources. This document must include:

a) A finalized Contractor Governance Model (as per section 2.1), introducing the participating individuals and their roles and responsibilities and how they will work within the SSC Project Governance; and
b) A finalized Contractor Core Delivery Team (as per section 2.3), introducing the key resources and their roles and responsibilities and how they will work with SSC's Project Team;
c) Onboarding initial Contractor resources will take place once the Contractor Core Delivery Team plan is accepted by SSC's Project Team.

5.1.3 Deliverable #3: Quality Management (QM) Plan

The Contractor must develop a QM Plan and obtain SSC PM acceptance in accordance with the requirements set out in section 2.8.

5.1.4 Deliverable #4: Risk Management (RM) Plan

The Contractor must develop a RM Plan and obtain SSC PM acceptance in accordance with the requirements set out in section 2.9.

5.1.5 Deliverable #5: Deliverable Review and Acceptance Process

The Contractor must develop, in collaboration with SSC, a Deliverable Review and Acceptance Process, and obtain SSC PM acceptance in accordance with the requirements set out in section 2.10.

5.1.6 Deliverable #6: Release Management Strategy

The Contractor must develop a Release Management Strategy for SSC acceptance. The Release Management Strategy must support SSC's envisioned collaborative process for ITSM Process Design and Tool Configuration and the ITSM Tool Implementation requirements in section 7.

5.1.7 Deliverable #7: Provide Hardware specifications for Release Management Strategy

The Contractor must develop the Hardware Specifications, in accordance with section 4.1, for the required Training environment for SSC acceptance.

5.1.8 Deliverable #8: Develop CWP&S

a) The Contractor must develop the Contractor Work Plan and Schedule (CWP&S) as set-out in section 2.5. The CWP&S must reflect the Contract award date, any input provided by SSC after Contract award, any mutually agreed to changes resulting from Deliverable #1, the agreed upon Rules of Engagement, Deliverable Review and Acceptance Process, and Release Management Strategy (Deliverables #2, 5, and 6 respectively), and further elaborated to provide schedule of completion of the initial agreed upon Work and clearly identify the tasks, milestones, deliverables, interdependencies and critical path.

b) The CWP&S must be submitted for SSC PM acceptance within 90 days of Contract award. The accepted CWP&S will be the baseline for the Contract.

6 DATA MIGRATION REQUIREMENTS

6.1 Approach

The legacy ITSM system (IBM Control Desk) and new ITSM Tool will co-exist for an indeterminate period of time. In accordance with best practices, existing incident, service request and change request records will not be moved from the legacy system to the new Tool.

Data migration and/or data creation activities to support implementation of the ITSM Tool Solution may be approached as follows:

- SSC must have the option to either migrate or create foundation data, including location and people (users, employees and customers) in the new Tool. (Note: There are over 15,000 user accounts in the ECD legacy tool, however there are only 4,000 staff in SSC using ECD. Therefore rather than investing in the clean-up of existing accounts, SSC believes it would be more efficient to create new user accounts in the new Tool.)
- Configuration Item (CI) and classification data must be migrated from the existing Configuration Management Database (CMDB) in the legacy tool to the new Tool. CMDB data will be staged and the staging area must be connected to the new Tool for feed of cleansed CI data.
- People groups and members data must be migrated to the new ITSM Tool.

6.2 Contractor Requirements

Further to the high level approach described above, the Contractor is responsible for migrating data to the new ITSM Tool including the following work:

6.2.1 Data Requirements for the ITSM Tool

The Contractor must, as and when requested, identify and document the data requirements for the new ITSM Tool. The Data Requirements must be documented and submitted within 30 days of the completion of Contactor Onboarding (set out in section 5). Following acceptance of the Data Requirements for the ITSM Tool, the Contractor must work with SSC to develop the scope of work for the subsequent Development of Data Migration Plan.

6.2.2 Development of Data Migration Plan

The Contractor must, as and when requested, collaborate with SSC to develop the detailed strategy and plan for how migration and reconciliation processes will be used to achieve the data migration goals of each release of the ITSM Tool. Following acceptance of the Data Migration Plan, the Contractor must work with SSC to develop the scope of work for the subsequent Migrate Data phase work required to implement each release of the ITSM Tool as applicable.

6.2.3 Migrate Data

The Contractor must, as and when requested, complete data migration for each Release of the ITSM Tool, which must as a minimum include but is not limited to the following activities and deliverables:

a) Create the source / target mapping specifications;

b) Design and implement the migration and reconciliation processes best suited to the types of data sources being migrated from;

c) Execute the migration processes between data sources and the new ITSM Tool;

d) Reconcile the migrated data in the ITSM Tool against data sources. Reconciliation will include implementation and execution of the reconciliation process. This also includes reporting results of the reconciliation for SSC review and approval purposes as well as for providing information to the Contractor team responsible for migration process correction;

e) Correct the migration processes where required in order to fix reconciliation issues;

f) Repeat the execution of migration and reconciliation processes for validation that the migration process works wherein all migrated content, including rich text content, is preserved in its original form once migrated to the ITSM Tool;

g) Collaborate with the SSC team responsible for data migration readiness;

h) Execute all activities associated with final migration of production data into the ITSM Tool as part of each Release (where data migration is required); and.

i) Provide support for user acceptance testing.

7 ITSM TOOL IMPLEMENTATION REQUIREMENTS

7.1 Approach

The Contractor will lead the Work associated with the Tool Implementation Process, to be conducted in Releases, and will involve representatives from SSC and other contractors (if applicable) engaged by SSC to support Service Delivery Transformation efforts, as follows:

Tool Implementation Process		Responsibility		
Steps	**Description**	**ITSM Process Maturity Solution contractor**	**SSC**	**Contractor**
1. Functional Design Specification	The functional design specification is developed. This document specifies exactly how the functional requirements will be met by the ITSM Tool Solution (e.g. workflows, button actions, additional form fields, etc.). The functional design specification is reviewed with SSC and the ITSM Process Maturity Solution contractor; this may be an iterative process for complex requirements. JAD sessions (Joint Application Design) may be used to expedite this step. SSC must approve the Functional Design Specification prior to configuration. This document is used as input for all downstream development process steps.	Support	Approve	**Lead**
2. Configuration/ Development Phase	The functional requirements are implemented in the ITSM Tool Solution according to the functional design specification. Depending on the features being implemented, oversight and approval may be required by SSC. Unit testing is completed in this step.	Support	Support (Approve if applicable)	**Lead**
3. Alpha demo	Newly implemented functional requirements are demonstrated to stakeholders to gain early feedback in advance of formal testing. The goal of this step is to ensure that the solution, as implemented, does in fact satisfy the functional requirements.	Support	Approve	**Lead**

	The development process may return to Step 1 or Step 2 following an alpha demo.			
4. Functional In-board Testing (FIT)	Integration testing done in the development environment to ensure that new features are functioning as expected and that it interoperates with other tools/applications as required.	-----	-----	**Lead**
5. System Integration Testing (SIT)	System testing done in the test environment where application is run through a test suite to ensure that overall system functionality is not broken.	Support	Approve	**Lead**
6. User Acceptance Testing (UAT)	End-to-end testing done in the test environment, by the customer, where the application is run through a test suite (end-to-end) to ensure that overall functionality is not broken and business requirements/processes are supported.	Support	**Lead** & Approve	Support
7. Deploy to Production	SSC provides oversight for the technical implementation of new functionality and manages all supporting business planning and Organizational Change Management (OCM) activities. The Contractor manages the technical aspects of the implementation of new functionality in Production: • Raising the necessary SSC change request(s) • Coordinating with other technical teams as required • Following SSC's change management processes • Deploying the configuration changes to Production • Communicating with identified stakeholders, change coordinators re: the status of the change	Support	**Lead** & Approve (provide Tier-1 support and trouble-shooting)	Apply changes to production & Provide Tier-2 support

The Requirements Management process for ITSM processes and associated Tool functionality will be managed by SSC and supported by the Contractor.

SSC will periodically provide the Contractor with packages of GC-specific ITSM process requirements and workflows to be implemented in the ITSM Tool. The level of effort and time required to configure each release of the ITSM Tool will be variable, depending on the quantity and complexity of the requirements contained in any given Release.

The Contractor must, as and when requested, implement the package into the Testing Environment of the ITSM Tool Solution within the cost and schedule parameters identified by SSC.

The Work to be conducted by the Contractor to support the Tool Implementation Process must include:

- Participation in ITSM Tool Release Planning and Management, in conjunction with SSC
- Consultation with SSC and ITSM Process Maturity Solution contractor stakeholders (as required)
- Development of Design Specifications
- Configuration of the Tool
- Conduct demonstrations and/or facilitate JAD sessions
- Testing
- Packaging for Deployment

The required Work is described in more detail in the sections that follow. The same activities and deliverables are associated with each Release, as and when requested by SSC.

7.2 ITSM Tool Release Planning and Management

The Contractor must develop and maintain an ITSM Tool Roadmap (i.e. Release Management Plan) that identifies any key dependencies between requirements or types of requirements that will have an impact on the composition of releases and sequence of implementation of certain requirements. The Roadmap must be maintained and kept current over the duration of the contract and reviewed with SSC as part of the ITSM Tool release planning activities.

The Contractor must ensuring that SSC is aware of the ITSM Tool Roadmap during the negotiation, planning and execution of each ITSM Tool Release. For Releases involving the implementation of ITSM process functional requirements, these requirements will be prioritised by SSC jointly with the Contractor.

Releases must incorporate, but not be limited to, the following activities:

a) Validate, negotiate and refine the requirements for each release;

b) Develop and deliver the high level architecture for each release including integration requirements with common components;

c) Develop the release plan;

d) Develop the proposed schedule and cost estimates to configure each release; and

e) Work with the SSC PM to develop a scope of work for the subsequent Development, Configuration, Testing and Deployment Phase work required to implement each release.

7.3 Consultation with SSC and ITSM Process Evolution Stakeholders

The Contractor must consult with various stakeholders at SSC to ensure that all requirements, regardless of type, are fully understood. In the case of functional requirements supporting ITSM process configuration,

the Contractor will participate in a collaborative process involving SSC and other contractors engaged by SSC to support Service Delivery Transformation efforts (e.g. ITSM Process Maturity Solution contractor).

7.4 Development of Design Specifications

The Contractor must produce Design Specifications for all implementation or configuration activities. Design specifications must be traced back to the corresponding requirements. The Contractor must, to the extent possible and as agreed by SSC, leverage configuration settings that are available in the ITSM Tool to address SSC's functional requirements rather than customizing the software. In cases where implementation or configuration work is necessary but cannot be attributed to one or more specific requirements, the Contractor must inform SSC.

In the case of functional requirements supporting ITSM process configuration, requirements will be provided in Process Configuration Requirements Specifications, which will be developed by the ITSM Process Maturity Solution contractor and approved by SSC.

Any specification involving user-facing functionality must incorporate usability specifications.

7.5 Configuration of the Tool

7.5.1 Contractor Configuration Requirements

7.5.1.1 Configuration Activities and Deliverables

The Contractor must configure the ITSM Tool, for each Release, including but not limited to the following activities and deliverables:

a) Provide input and/or guidance during the development of Process Configuration Requirement Specifications as and when required.

b) Provide input into the Requirements Management process as and when required.

c) Provide input into the Release Planning process as and when needed.

d) Review all approved Requirements Specifications provided by SSC, and perform the following tasks when applicable:

   I. Identify questions and seek clarification regarding the Requirements Specifications.

   II. Identify upstream or downstream dependencies pertaining to the requirements contained in the Requirements Specification. Dependencies are not limited to ITSM Tool functionality and may include, for example, training, ITSM Tool licensing, ITSM Tool infrastructure and subject matter experts.

   III. Identify gaps between requirements contained in the Requirements Specification and the ITSM Tool capabilities. For each gap identified, the Contractor must provide all reasonable options to address the gap, along with costs and impacts to schedule.

e) Identify when there is more than one way to meet the Requirements in the ITSM Tool. When asked to do so by SSC, the Contractor is responsible for coordinating and facilitating options analysis workshops and/or proof of concept demos with SSC stakeholders in order to identify the preferred approach.

f) Produce Functional Design Specification document(s) that will identify how each requirement will be met by the ITSM Tool, including user experience (UX) designs when applicable.

g) Obtain SSC's approval of the Functional Design Specification prior to performing Tool configuration activities (excluding configuration to support demos or proof of concept).

h) Configure the ITSM Tool according to the Functional Design Specification.

i) Develop the system security controls for each Release;

j) Package the configuration changes in accordance with section 7.8.

k) Create the system load profiles (e.g. daily, quarterly, etc.) to be used to ensure that the system performs in accordance with the non-functional requirements under these load conditions.

l) Test (Unit, SIT, Performance/Stress, UAT support).Produce a technical cutover plan in alignment with SSC's Change and Release management policies that integrates with the ITSM Process Maturity Contractor's Deployment Plan.

m) Planning and execution of any data migration and conversion required in order to meet the requirements contained in the Requirements Specification.

7.5.1.2 Integration Configuration

The Contractor must, as and when requested, implement the integrations as identified in section 8, Integration Requirements.

7.5.1.3 Configuration Recommendations and Advice

a) The Contractor must provide recommendations and advice to SSC, related to the ITSM Tool, in order to leverage the out-of-the box functionality and minimize the level of customization of the Tool.

b) In cases where SSC business requirements cannot be met to SSC's satisfaction, through configuration (as defined in Appendix 3), the Contractor must propose alternative solution(s) (including customization) along with any associated costs, risks, dependencies and impacts to schedule for SSC approval prior to proceeding.

7.6 Testing

For each Release, the Contractor must conduct all necessary testing to ensure the release will pass subsequent acceptance tests at SSC. Refer to section 9 for detailed System Testing requirements.

The Contractor is responsible for completing and verifying the migration of the release components to the test environment. Migrations of Contractor deliverables into the SSC test environment must be done by the Contractor in accordance with the agreed upon Deliverable Review and Acceptance Process developed during Contractor Onboarding (refer to section 5).

After the Contractor has verified successful migration, SSC resources will perform acceptance tests of the released ITSM Tool Solution. Any errors identified during the acceptance testing must be corrected by the Contractor at no additional cost to SSC in accordance with the Deliverable Review and Acceptance Process to be agreed to by SSC and the Contractor. The final such release will indicate readiness to release to the SSC production environment.

7.7 Packaging for Deployment

Any changes to the ITSM test or production environments must be done through the application of testable and repeatable deployment packages. There may not be any changes made to the production environment that had not previously applied to the test environment without SSC's written approval.

7.7.1 Software Development Lifecycle (SDLC)

The Contractor must implement and follow a SDLC to be agreed with SSC during the Contractor Onboarding phase of the contract. The SDLC must ensure that all configuration and customization changes to the ITSM Tool Solution are applied and packaged in a standard way that will minimize risk to the ITSM Tool Solution integrity in the production environment.

The SDLC must include a configuration management plan for tracking ITSM and related software versions, as well as packages, in all environments.

7.7.2 Packaging for Test Environment

For the purposes of packaging, the test environment must be treated as a “pre-production” environment. The SDLC must ensure that all packages destined for production are first applied to, and tested in, the test environment.

7.7.3 Packaging for Production Environment

In order for a package to be applied to the production environment, it must be identical to the package that has most recently been applied to the test environment. If a situation arises where a package must be applied to the production environment that differs from the package used in the test environment, the Contractor must obtain written approval from the SSC PM prior to doing so.

7.7.4 Package Contents

The package must include all artifacts required to apply the package in the target environment. The package should be written and assembled in such a way that the package can be applied by an individual with no working knowledge of the package contents (e.g. ITSM Operations team). In cases where specialist skills are required to apply the package, the package must state this clearly.

Each package must contain, but is not limited to, the following artifacts:

1. Method of procedures – a detailed set of instructions (including any prerequisite conditions) to be followed by the individual applying the package to the target environment. All manual and automated steps must be documented.
2. Package artifacts – any file or other artifact required to support the application of the package in the target environment. (E.g. configuration files, code modules, data files to be imported, etc.)
3. Back out procedures – to be used if problems are encountered during the application of the package.
4. Verification test scripts – test scripts used to verify that the package has been applied correctly.

8 INTEGRATION REQUIREMENTS

8.1 General Integration Requirements

Each integration to be delivered by the Contractor must support the following requirements:

- Provide a user interface for administering the integration infrastructure.
- Business rules should be configurable whenever possible. Hard-coding of business rules (including data transformation) should be avoided.

- Provide a mechanism to monitor the interface for errors, failures and performance issues.

The Contractor must, as and when requested, implement an integration solution for the new ITSM Tool Solution.

8.2 Integration with SSC Applications

The Work associated with the implementation of the new ITSM Tool Solution involves a significant integration component, including:

a) The development of a holistic integration strategy which will establish standards for the exchange of information and may, in the future, leverage GC Service Bus (i.e. Oracle Service Bus);

b) The design and implementation of a standards-based bi-directional interface which adheres to SSC's ITSM Data Standards to support the exchange of data between SSC's new ITSM Tool and the ITSM tool(s) in use at the customer;

c) The implementation of interim interoperability solution between the new ITSM Tool and SSC's existing ITSM toolset in order to ensure business continuity until such time as the functionality from those legacy tools is replaced by the new Tool; and

d) The implementation of interfaces between the new ITSM Tool and required SSC corporate systems.

Integrations between the ITSM Tool Solution and other SSC and GC applications must be delivered by the Contractor, as and when requested. The long term integration solution will be implemented on a phased basis and some legacy integrations will remain until such time as they can be replaced.

8.3 Interoperability with GC Customer ITSM tools

8.3.1 Bi-directional Interface Requirements

The ITSM Tool Solution must implement the infrastructure, technology and business rules (i.e. "an interface") to support bi-directional communication and passing of data between SSC's ITSM Tool Solution and the ITSM tools of other GC Customer departments. Across government there is a wide range of ITSM tools and versions in use.

The ITSM Tool Solution must support:

1. Interface between tenants on SSC's multi-tenant ITSM instance
2. Interface between other GC Customer departmental ITSM tools and SSC's multi-tenant ITSM instance, where the customer department is using the same Toolset as SSC.
3. Interface between other GC Customer departmental ITSM tools (including multi-tenant instances) and SSC's multi-tenant ITSM instance, where the customer department is using a different ITSM Tool than SSC.

In addition, the ITSM Tool Solution must:

- Provide a standardized, documented set of operations and data attributes, which can be consumed by SSC and OGDs, and which adhere to the ITSM Data Standards in place at that time (draft version provided in Attachment 3).
- Support updates to a single record or multiple records in a single transaction.

9 SYSTEM TESTING REQUIREMENTS

9.1 Contractor Testing Requirements

The Contractor must participate in the various types of ITSM Tool Solution testing in accordance with the type of testing, roles and responsibilities identified in section 7.1. For those testing activities for which the Contractor has been identified as the Lead, the Contractor must provide:

a) Testing processes

b) Testing personnel

c) Testing tools and scripts

9.2 Unit Testing

The Contractor must conduct unit testing for any coded or configured deliverables prior to releasing for FIT testing as set out in section 7.1.

9.2.1 FIT Testing (Functional In-board Testing)

The Contractor must define, implement and coordinate the FIT testing process for each Release.

9.2.2 SIT Testing (System Integration Testing)

The Contractor must define, implement and coordinate the SIT testing process for each Release. SIT must include at minimum, the following application performance testing types: load testing and stress testing whereby Load testing objective is to identify application performance under anticipated user loads and stress testing will test the application under extreme workloads to validate high traffic or data processing.

9.2.3 UAT (User Acceptance Testing)

a) The Contractor must support the UAT process, which will be implemented and managed by SSC, for each Release.

b) Once a Process has been configured into the ITSM Tool and delivered to SSC in the Testing Environment, SSC will review and provide acceptance within 15 business days.

c) In the event that SSC discovers an issue, SSC will provide feedback to the Contractor within 15 business days. The Contractor must then investigate the issue within 48 hours and provide a time estimate as to its resolution, and address the issue accordingly.

d) After SSC has accepted the Process as configured and tested in the Testing Environment, the Contractor will have 15 business days to implement that process into the production environment.

10 TRAINING SERVICES REQUIREMENTS

The Contractor must, as and when requested, provide Training Services which may include any of the following:

10.1 ITSM Tool Orientation Sessions

The Contractor must prepare and conduct ITSM Tool Orientation Sessions that will provide ITSM Process Evolution initiative stakeholders sufficient training on the ITSM Tool so that they understand the overall structure and layout of the application and its modules.

The ITSM Tool Orientation sessions will be delivered on a minimum of four occasions in order to train approximately 100 stakeholders including:

- 30 from ITSM process areas
- 5 from ITSM Tool Project Team
- 50 from Process Maturity Team, including the ITSM Process Maturity Solution contractor
- 15 other

Attendees must complete the ITSM Tool Orientation sessions with sufficient understanding of the ITSM Tool so they can effectively continue business analysis and process evaluation activities. Topics to be included in the ITSM Tool Orientation Session should include, but are not limited to:

a) Overall application layout and navigation

b) Permission/Role structure, and how this drives Tool behavior

c) How each type of ITSM record is managed and carried through its lifecycle

d) An overview of workflow configuration capabilities (Approvals, ticket routing, etc.)

e) How the consoles (queues) can be leveraged by support staff, managers

f) How dashboards can be viewed and configured by various roles

g) Self-service portal navigation and features

h) Reporting – User-configurable reports, consuming and publishing reports

i) An overview of the ITSM data model, identifying the key data sources and dependencies that support the Tool functionality in each process.

The ITSM Tool Orientation Sessions must be classroom-based in the National Capital Region (NCR - Ottawa and Gatineau), with a virtual option for off-site staff. Each session must be provided in English or French as requested by SSC. The Contractor must provide all course materials which can be retained by attendees for future reference.

10.2 Process Administrator Training

The Contractor must, as and when requested, prepare and conduct training for SSC stakeholders assigned process administrative responsibilities (i.e. Business Systems Analyst resources) such as workflow configuration, self-service portal updates, report creation, etc. This training must be classroom based in the NCR, with a virtual option for off-site staff, and available on an ad-hoc basis with agreed notice. The content of each training course will be discussed with the Contractor and agreed upon prior to

delivery of training. The curriculum must cover process configuration topics that do not require system level access or coding knowledge.

It is recognized that some topics will only be appropriate once SSC is familiar with how the ITSM processes have been configured within the Tool.

10.3 ITSM Tool System Administrator Training

The Contractor must, as and when requested, prepare and conduct training for ITSM Tool System Administrators (i.e. Technical resources that support the application) if training requirements, identified under the Transition Plan (set out in section 12) cannot be fulfilled by third-party Training providers. .

10.4 ITSM Process and Tool Training

The Contractor must, as and when requested, provide materials (e.g. user manuals, video tutorials, etc.) and training to SSC staff (train-the-trainers) that will, in turn, be responsible for the development and delivery of ITSM process and Tool training to SSC employees. The material and training must provide sufficient understanding of the overall structure and layout of the application, its modules and its use within SSC so that SSC staff can develop SSC specific training materials for internal use. This training may have to be delivered on multiple occasions and must be classroom-based in the National Capital Region (NCR - Ottawa and Gatineau) with a virtual option for off-site staff, and available on an ad-hoc basis with agreed notice.

10.5 Classroom Training

All classroom training must adhere to the following conditions:

a) Each classroom training session may include up to a maximum of 20 students;

b) Classroom training must be provided in the NCR. The classroom training locations may be modified on a case-by-case basis, subject to the consent of the SSC PM.

c) Classroom training must include a virtual option for off-site staff. Virtual training to be provided according to industry standards (e.g. WebEx, GoToMeeting, etc.).

d) All training materials must be delivered in accordance with GC Standards for Accessibility.

e) Any exceptions to classroom training must be approved by the SSC PM.

10.6 Required Training Materials

a) The Contractor must provide the SSC Project Manager with all training materials, in English ~~and~~or French, for review and acceptance no less than twenty business days prior to the start of any training course. SSC will provide its approval or any comments for change within ten business days. The Contractor must address those comments before using the materials for training~~.~~ and translate as required. Final versions of all training material in English and French must be completed and shared with SSC no less than five business days prior to the start of any training course.

b) All training materials provided by the Contractor must include:

a. a course syllabus;

b. a course schedule; and

c. courseware and training materials for the applicable training course.

c) For each training course, both the instruction and the course materials must be available in either English or French, or both, as specified by SSC.

d) In addition, the Contractor must provide a video recording of each of the four types of training sessions (10.1-10.4 above), as applicable, for future SSC use (e.g. publish on SSC portal).

11 AD-HOC PROFESSIONAL SERVICES REQUIREMENTS

In addition to the Work described herein SSC may, on an as and when requested basis, require that the Contractor provide additional professional services to support SSC in the implementation of the ITSM Tool Solution within the SSC environment as well as support customer departments to onboard to SSC's instance of the ITSM Tool Solution and/or configure their own instance of the Tool. Ad-hoc professional services, if requested, would be limited to the resource categories listed in SOW section 2.12.

12 TRANSITION OUT SERVICES REQUIREMENTS

The Contractor must support the ITSM Tool Solution, as set out in section 13. SSC, at its option, will transition responsibility for management of the ITSM Tool Solution at a future date. The Contractor must, as and when requested, provide Transition Out Services to enable SSC to assume responsibility for the entire ITSM Tool Solution including, but not limited to, configuration of the Tool and application management and operations.

Transition Out requirements are more fully described in the sections that follow.

12.1 Transition Plan

The Contractor must, as and when requested, develop a Transition Plan that covers the transitioning of management of the ITSM Tool Solution to SSC. All aspects of the ITSM Tool Solution for which the Tool Contractor is responsible for delivering as per this SOW must be included in the Transition Plan.

The development of the Transition Plan must be completed in accordance with the Detailed Work Plan for Development of Transition Out Plan contained in the Contractor's Bid and must include, but is not limited to, the following topics:

12.1.1 Resource Plan

The Transition Plan must include a comprehensive resource plan that will form the basis of SSC's staffing requirements. The plan will be developed in collaboration with SSC to ensure alignment with SSC organizational structure and GC HR policies and should include all roles involved with the ITSM Tool Solution and their respective responsibilities and accountabilities.

12.1.2 Training/Certification Plan

The Transition Plan must include a list of training and/or certification courses that SSC staff, acting in the roles identified in the Resource Pan, will need to attend or obtain as part of the transition process.

12.1.3 Knowledge Transfer Plan

The Transition Plan must include a register of all required knowledge transfer topics, including supporting documentation, which SSC stakeholders will require. The plan must also propose a schedule for conducting knowledge transfer sessions with identified stakeholders and include validation criteria to confirm the knowledge transfer was successful and measure its effectiveness over time.

12.1.4 Documentation Plan

The Transition Plan must provide SSC with a comprehensive package of material to support the transition and provide the basis of the ITSM Tool documentation library moving forward. This package should include, but is not limited to the following:

a) Solution architecture diagram(s) depicting the entire ITSM Tool Solution, including integrations with upstream and downstream systems, hardware and software components, network connectivity, High Availability infrastructure, security devices, etc.

b) Catalogue of all SSC provided ITSM Tool related hardware components, with a description of each.

c) Catalogue of all ITSM Tool related software, middleware and database components with detailed descriptions of each, along with version/patch information.

d) A runbook/manual with detailed step-by-step instructions for installing a new instance of the ITSM Tool software on a new server and applying all configurations required for use at SSC.

e) Lessons learned registry

f) Known error registry/database

g) Catalogue of all configurations made to each ITSM Tool Solution component

h) Catalogue of all configuration settings made to the ITSM application (including any configuration file/server settings)

i) Catalogue of all integrations, with corresponding settings and account information.

j) Catalogue of any customizations to the ITSM Tool, with detailed listing of customized/overlaid objects or code.

k) Start-of-day manual, documenting start of day or any other periodic procedures to be performed on the ITSM Tool and/or supporting components.

l) Disaster Recovery plan

m) Processes and procedures for the support of the ITSM Tool (Operating Model)

n) Software Development Lifecycle (SDLC) best practices for packaging ITSM Tool configuration changes and applying them to other ITSM environments.

12.1.5 Operational Readiness Plan

The Contractor must include a plan for ensuring that the identified SSC staff/teams are able to manage their work from inside the ITSM Tool. This includes a plan for setting up all of the necessary SSC Resolver Groups and members, user accounts, ticket routing rules and SLAs to allow SSC staff to manage requests, incidents, changes, releases, problems, CIs and knowledge base content associated with the ITSM Tool Solution, in alignment with the CONOPS.

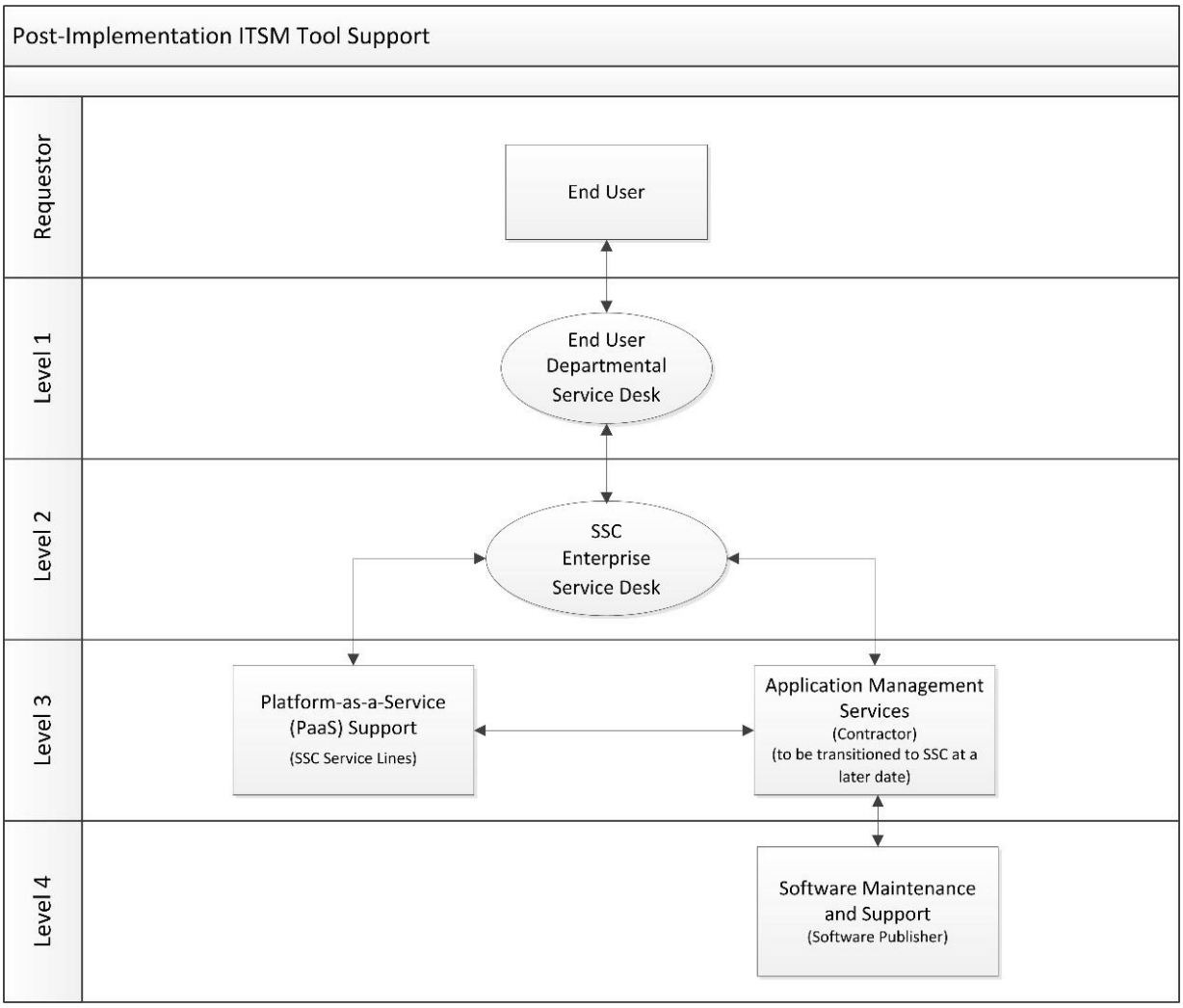
12.2 Execution of Transition Plan

The Contractor must, as and when requested, execute the Transition Plan.

13 APPLICATION MANAGEMENT SUPPORT

13.1 Post-Implementation Support Model

Post-implementation, the ITSM Tool Solution will be supported in accordance with SSC's desk-to-desk support model as depicted in the graphic below:



- **1st Level Support**
  1st level support will be provided by the end-user's departmental service desk.

  ITSM End-users submitting requests related to the ITSM Tool Solution or experiencing issues with the Tool will contact their departmental service desk. Through initial diagnosis, if it is determined that the end user's issue (incident) or request is related to the ITSM Tool Solution, the departmental service desk will escalate the incident or request to 2nd level support: SSC's Enterprise Service Desk.

- **2nd Level Support**
  2nd level support will be provided by SSC's Enterprise Service Desk.

  Upon receipt of an ITSM Tool Solution incident or request, SSC's Enterprise Service Desk will perform further diagnosis and try to resolve the incident or fulfill the request. Incidents or requests that cannot be resolved/fulfilled will be escalated to 3rd level support for resolution as follows:

  - SSC Service Line(s) Support for hardware infrastructure related incidents or requests (e.g. hardware, middleware, OS, storage, network, etc.), or
  - Application Management Support for application related incident or requests.

- **3rd Level Support**
  3rd Level support will be provided by as applicable by:

  - SSC Service Line staff for hardware infrastructure related incidents, service requests and change requests and/or
  - The Contractor (until such time as transitioned to SSC) Application Management Support for application related incidents, problems, service requests and change requests. If it is determined that there is an ITSM Tool software related incident, 3rd level support will escalate to 4th level support.

- **4th Level Support**
  4th level support for ITSM Tool Solution related incidents will be provided by the Contractor.

13.2 Hypercare Support Services

13.2.1 Hypercare

The Contractor must, if and when requested, perform Hypercare Support Services for each Release of the ITSM Tool Solution with a particular, but not exclusive, focus on customer support and Incident responsiveness, system and data integrity and system availability.

If requested, Hypercare Services may include:

a) Successful Performance testing including load and stress testing of the ITSM Tool Solution (after each Release) against applicable Service Level Objectives (SLOs) as identified at the time of request. The Contractor must identify if any corrective action is required, by the Contractor or SSC, to maintain the identified SLOs and take corrective action as applicable.

b) Increased levels of support services, as established between SSC and the Contractor at the time of the request, which are over and above routine AMS operational support levels to manage the typical increase in system Incidents and customer support calls immediately following production implementation of a new release.

13.2.2 Hypercare – By Release

For the Initial Release, as well as subsequent Releases of the ITSM Tool Solution, Hypercare Support Services must be provided, if and when requested, after production implementation of the Release until such time that the following conditions are met:

1) At least one financial month-end has completed without any Critical (i.e. Severity 1) Incidents being raised during month-end processing;
2) All data migrations have been completed;
3) All system interfaces to and from the ITSM Tool Solution have completed a pre-determined representative sample of processing in production at least once without any Critical (i.e. Severity 1) or High (i.e. Severity 2) Incidents;
4) There are no open Critical or High Incidents related to the Release;
5) The "Measuring Impact - Post- implementation evaluation and remediation" activities and Deliverables must be completed; and
6) The identified Service Level Objectives (SLOs), as applicable, have been met and SSC Project Manager approval received to conclude Hypercare and proceed into Application Management Services (as defined in 13.3).

13.3 Application Management Support Service Requirements

13.3.1 Application Management Services

a) 3rd Level Application Management Services, relating to the ITSM Tool Solution (including interfaces) that have been implemented under the Contract, to be provided must include but are not limited to the following tasks and activities and must be carried out using SSC's instance of the ITSM Tool Solution:

   a. Monitor all applicable ITSM queues within the ITSM Tool Solution for application related incidents, service requests, problems and change requests;

   b. Respond to, resolve and manage incidents and any related problems according to established Service Level Agreements in accordance with SSC processes, policies and procedures for Incident and Problem Management;

   c. Record, within the ITSM Tool, all steps taken to investigate the cause of an incident or problem record prior to reassigning it to an SSC Resolver Group;

   d. Escalate incidents and problems to the appropriate support levels within the Contractor and the ITSM Tool Software Publisher, if applicable;

   e. Create and apply patches for the ITSM Tool Solution, subject to SSC written authorization, for incidents and problems that have been escalated to the ITSM Tool Software Publisher for 4th Level Support. Any patches created and applied to the ITSM Tool Solution by the Contractor must be backed out and replaced by patches from the ITSM Tool Software Publisher when they become available;

   f. Contribute to the fulfillment of service requests in accordance with SSC processes, policies and procedures for Request Fulfillment;

   g. Initiate and contribute to all phases of change requests when changes to the ITSM Tool Solution are required, in accordance with SSC processes, policies and procedures for Change Management;

h. Create and maintain a model of the ITSM Tool Solution in the ITSM Tool's CMDB that represents all ITSM environments, including supporting infrastructure and all dependency relationships. SSC will be responsible for providing information pertaining to the infrastructure. The Contractor will be responsible for maintaining the accuracy of those components of the model pertaining to the ITSM Tool, middleware, database and integration components, through adherence to SSC's Service Asset and Configuration Management (SACM) process;

i. Participate in SSC Change Advisory Board (CAB) meetings as required;

j. Lead post-installation reviews and lessons-learned workshops following the implementation of change requests and releases, if requested;

k. Provide regular status reports for any escalated incidents, problems and service requests;

l. Perform regular performance tuning (ITSM Tool, database, middleware, integrations) to achieve the stipulated service levels;

m. Planning and execution of patching for all ITSM Tool Solution related components (ITSM Tool, database, middleware);

n. ITSM Tool database administration and support;

o. Lead regular ITSM Tool Solution capacity planning activities in conjunction with SSC Service Lines (infrastructure, facilities, networks), and the ITSM Tool business owner;

p. Provide ITSM Tool, database and middleware product roadmaps and facilitate ITSM Tool Solution upgrade planning activities in conjunction with SSC Service Lines and the ITSM Tool business owner;

q. Create, maintain and provide SSC access to ITSM Tool Solution Architecture Diagram(s);

r. Create and maintain ITSM Tool Solution run books (installation run books, system configuration settings, etc.); and

s. Create and maintain an ITSM Tool Solution knowledge database, including lessons learned over the duration of the contract, within the ITSM Tool's Knowledge Management module. The knowledge database must be available for searching by SSC staff with the appropriate permissions, and become the property of SSC when 3rd Level Support of the ITSM Tool Solution transitions to SSC.

b) The Contractor's AMS support resources must possess the knowledge and experience to deliver the services required under this Contract. The Contractor must provide training for its technical support resources relating to the SSC environment and on the specifics of the ITSM Tool Solution implementation for SSC.

13.3.2 AMS Requirements

a) The Contractor must provide 3rd Level AMS services (as per section 13.3.1) for a period of one-year, following the conclusion of the Hypercare period.

b) The Contractor must, if and when requested, conduct Transition out activities (as set out in section 12) in order to transition responsibility for AMS from the Contractor to SSC's application management support team.

13.3.3 Optional to extend AMS

a) The Contractor must, if and when requested, provide 3rd Level AMS services (as per section 13.3.1) for up to nine additional one- year periods.

b) The Contractor must, if and when requested, conduct Transition activities (as set out in section 12) in order to transition responsibility for AMS from the Contractor to SSC's application management support team.

APPENDIX 1 – ITSM TOOL NON-FUNCTIONAL REQUIREMENTS

This Appendix sets out the mandatory non-functional requirements that the ITSM Tool, and ITSM Tool Solution implemented by the Contractor, must meet.

1 PLATFORM DEPLOYMENT

NFR-1	Platform	
NFR-1.1	Platform Deployment	a) The ITSM Tool must have the capability to be installed and run within GC Enterprise Data Centres and the zoned networks therein. b) The ITSM Tool Solution implemented by the Contractor must be fully supported by the Software Publisher in an on premise deployment model.

2 INTENTIONALLY LEFT BLANK

3 BACKUP AND RESTORE

NFR-3	Data Backups	
NFR-3.2.	Backup Restore	The ITSM Tool Solution implemented by the Contractor, or data associated with the ITSM Tool Solution, must have the capability to be backed up and restored to any previous backup (i.e. recovery point).

4 HIGH AVAILABILITY AND DISASTER RECOVERY

NFR-4	High Availability and Disaster Recovery	
NFR-4.1	High Availability	The ITSM Tool must have the capability to support a high availability architecture using techniques such as clustering and load balancing.
NFR-4.2	Disaster Recovery	The ITSM Tool must have the capability to support disaster recovery across multiple data centres through an active-passive model.

5 SUPPORTABILITY

NFR-5	Supportability	
NFR-5.2	Portability	The ITSM Tool must have the capability to be copied or moved to a completely separate set of infrastructure providing the same functionality and service as the source ITSM instance.
NFR-5.3	Auditability	The ITSM Tool must have the capability to record and provide the following information at all times, including when the ITSM Tool Solution is unavailable (unless otherwise specified): a) All system warnings and errors over the previous 72 hours for all components of the ITSM Tool Solution; b) Currently logged in users (only applies when ITSM Tool Solution is available); and c) All login attempts for previous 90 days.
NFR-5.5	Configurability in live environments	The ITSM Tool must have the capability to be configured in a way that does not require service outages or downtime. This includes, at a minimum, adding, updating or removing the following types of configuration: a) Incident, Request, Change Request, Problem and CMDB record classification data (Impact/Urgency/Categorization) b) Request and Change Request approval workflows and rules c) Incident, Request, Change Request and Problem record auto-routing (assignment)rules d) Incident, Request and Change Request Service Level Targets e) Creating new form fields or hiding existing fields from view f) Service Catalogue data (E.g. new or updated information about service offerings which must be reflected on the self-service portal) g) Publishing of Knowledge Articles and FAQs h) Adding, changing, or removing notifications (including notification content) i) Adding or changing reports and their definitions/templates
NFR-5.6	Scalability	The ITSM Tool must have the capability to increase total output under an increased load when additional infrastructure capacity is added.

6 DATA ARCHIVING

NFR-6	Data Archiving	
NFR-6.1	ITSM Archiving Feature	a) The ITSM Tool Solution must include functionality to archive and retain ITSM records (e.g. Incidents, Service Requests, Tasks), and associated data such as attachments, to be accessed when required. b) The achieving functionality solution must be configurable in accordance with the customer's data retention policy.

7 PERFORMANCE AND CAPACITY

NFR-7	Performance & Capacity	
NFR-7.1	Capacity and Performance	The ITSM Tool must have the capability to support a response time objective of one second or less for non-resource intensive functions such as selecting menus, saving records or navigating to a different view or screen in the ITSM software.
NFR-7.2	Capacity and Performance	The ITSM Tool must have the capability to support a response time objective of three seconds or less for moderate-resource intensive functions, such as browsing the user's personal dashboard or queue, refreshing tables and results lists, searching knowledge base articles.
NFR-7.3	Capacity and Performance	The ITSM Tool must have the capability to support a response time objective of seven seconds or less for resource intensive functions, such as generating ad-hoc management reports.
NFR-7.5	Target Throughput (Production)	The ITSM Tool must have the capability to support NFR-7.1 to NFR-7.3 as Tool users are added and/or as additional processes are configured in the Tool over time.

8 SYSTEM INTERFACES

NFR-8	Interfaces	
NFR-8.1	Integration Methods	The ITSM Tool must support industry accepted open standards for integrating with other GC applications, including: • LDAP • API (C, Java, .Net, C#, etc.) • Representative State Transfer (REST) API • Web Services/Simple Object Access Protocol (SOAP) • JSON • XML • SAML • ODBC 3rd party applications must be able to use the standards listed above to interact with all ITSM application data entities, processes and workflows as required, and not be restricted to specific operations with the ITSM Tool.
NFR-8.2	Multiple LDAP Sources	The ITSM Tool software must be capable of connecting to multiple LDAP sources concurrently for user authentication and/or data extraction purposes.

9 INTENTIONALLY LEFT BLANK

10 SECURITY

NFR-10	Security	
NFR-10.1	Security Standards	The ITSM Tool and the ITSM Tool Solution implemented by the Contractor must adhere to the GC and SSC security policies and requirements as stipulated in the Security Controls contained in Appendix 4.
NFR-10.2	Email Security	The ITSM Tool's email integration capability must support TLS (Transport Layer Security).
NFR-10.3	Application layer responsibility	Where security controls are a shared responsibility between the infrastructure layers and application layers as stipulated in the Security Controls contained in Appendix 4; the Contractor is responsible for the security control at the application layer.
NFR-10.4	Network Zoning	The ITSM Tool and the ITSM Tool Solution implemented by the Contractor must adhere to the SSC defined network zoning guidelines as follows: a) Baseline Security Requirements for Network Security Zones in the Government of SSC https://www.cse-cst.gc.ca/en/publication/itsg-22

NFR-10	Security	
		b) Network Security https://cyber.gc.ca/en/publications (Filter by topic: Network Security) c) ITSG 38 https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg-38-eng.pdf

11 USABILITY

NFR-11	Multi-Platform	
NFR-11.1	Multi-Platform Support (Web)	The ITSM Tool must support, at a minimum, the following commercial web browsers: a) Microsoft Internet Explorer (current and subsequent versions); b) Google Chrome (current and subsequent versions); and c) Mozilla Firefox (current and subsequent versions).
NFR-11.2	Multi-Platform Support (Mobile/Tablet)	The ITSM Tool must support mobile and tablet devices for the following functionality: a) Service request and change request approvals, rejections and comments; b) Notification of ticket assignment; c) Monitoring of incident, service request and change request queues; d) Creation and update of incident, service requests and change requests; and e) View dashboards and reports.

12 USER INTERFACE

NFR-12	User Interface	
NFR-12.1.	Localization	The ITSM Tool must have the capability to support both Canadian English and Canadian French, based on individual users' preferences. Localised functionality must include, but is not limited to, the following: a) All ITSM screens accessible by end users; b) All notification content; c) Reports; d) Knowledge Articles and FAQs; and

		e) Self Service Portal and Service Catalogue.
NFR-12.2	Federal Identity Program	The ITSM Tool must provide a Self-Service Portal which complies with the TBS FIP standard at the time of Contract Award. The FIP standard can be found at: http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/fip-pcim/index-eng.asp
NFR-12.3	Web Accessibility	The ITSM Tool must comply with WCAG 2.0. The WCAG 2.0 requirements can be found at: www.w3.org/WAI/standards-guidelines/wcag/
NFR-12.4	Web Usability	The ITSM Tool must comply with the Standard on Web Usability. The standard ensures Government of Canada websites and Web applications respect usability principles and approaches. The Standard on Web Usability can be found at: http://wwwtbs-sct.gc.ca/pol/doc-eng.aspx?id=24227

13 MULTI-TENANCY

NFR-13	**Multi-Tenancy**	
NFR-13.1	Multi-Tenancy	The ITSM Tool must have the capability to support multiple, independently configured and used, tenants on the same instance.
NFR-13.2	Access Control	The ITSM Tool must include functionality that allows administrators to provide user access controls within a multi-tenant environment, as follows: a) Users must only have access to view or update ITSM records, field selection values, menus, reports etc. that belong to the Tenant to which the users belong. b) Each Tenant can define and create specific users or user groups for their instance with appropriate permissions. c) Only a Tool Administrator can have access to multiple tenants.
NFR-13.3	Configuration	The ITSM Tool must provide a web based interface which has the capability to allow multiple Tenants to add and/or modify users and user groups for their specific organization.

14 TOOL EXTENSIBILITY

NFR-14	**Tool Extensibility**	
NFR-14.1	Extensibility	The ITSM Tool must have the capability to allow the following types of changes to be made:

NFR-14	Tool Extensibility	
		a) Addition of screens or forms that can be incorporated into the ITSM Tool's permission model b) Addition of custom business rules and/or workflows to the ITSM Tool c) Addition of fields to forms that were originally shipped with the ITSM Tool software d) Alterations to the layout of screens that were originally shipped with the ITSM Tool software. This includes, but is not limited to: 1. Making the screen larger or smaller 2. Moving fields that were shipped with the ITSM Tool software, or hiding them from view 3. Add or remove columns on tables or lists 4. Modification to the order in which columns appear in tables 5. Modification to the sort and/or qualification properties and columns of tables, lists and queues e) Incorporation of newly built screens/forms into the ITSM Tool software in such a way that it matches the ITSM Software look and feel and can be incorporated into the ITSM Software GUI navigation scheme.
NFR-14.2	Mobile	Any new or extended components (as described in NFR-14.1) must be automatically reflected in the ITSM Tool mobile device user interface.

15 DATABASE

NFR-15	Database	
NFR-15.1	Supported Database	The ITSM Tool must support one of the following databases: a) Microsoft SQL; or b) Oracle RDBMS.

APPENDIX 2 – ITSM TOOL FUNCTIONAL REQUIREMENTS

This Appendix sets out the mandatory functional requirements (e.g. the tasks, functions or actions) that the ITSM Tool Software, identified in the Contractor's Bid, must meet in order to support SSC's identified business requirements.

Note: The functional requirements identified in each of the sections that follow align with SSC's ITSM Process Evolution initiative.

1 GENERAL

Functional Requirements: General		
ID	**Name**	**Description**
FR-1.1	Bilingual	The ITSM Tool must include functionality that allows users to choose to work in English or French (e.g. fields, button, forms, selection lists, labels and notifications, help screens and mouse overs must be in the chosen language) and allow the user to toggle from French to English. The ITSM Tool software must also remember the user's chosen language preference.

FR-1.2	Search Capabilities	The ITSM Tool must include functionality that provides search capabilities in all ITSM processes including ad-hoc queries, save queries, user queries, role-based queries, shared/public queries.
		- Ad hoc queries (support/process staff)
		- Portal
		  ○ Search across service catalog
		  ○ Search across knowledge base articles/FAQs/bulletin board/broadcasts
		- Queues/consoles
		  ○ Saved searches
		  ○ Role based searches and views

FR-1.3	Integration with Customer ITSM Tools	The ITSM Tool must have the capability to support standardized processes and an ITSM Tool interface that enables bi-directional communication between SSC's Tool and customers' tool with smooth and continuous workflow to support and improve the quality delivery of services.
FR-1.4	Shared Ticket Visibility	The ITSM Tool must include functionality that provides customer/SSC visibility of shared ticket (e.g. incident, problem, change) and CI information to understand departmental-wide impacts/dependencies of outages, planned change activity, etc.
FR-1.5	Email	Users of the ITSM Tool must be able to create and update tickets (e.g. incidents, service requests, changes) via email.
FR-1.6	Voice Recognition	The ITSM Tool must have the capability to create a request or incident and update status through integration with Integrated Voice Recognition (IVR).
FR-1.7	ITSM User Categories	The ITSM Tool must include functionality that allows for the identification of user categories that will permit the separation of access and permissions.
FR-1.8	System Notifications	The ITSM Tool must include functionality that allows for the configuration of, at process level, when users should receive notifications from the system.
FR-1.9		*Intentionally left blank*

Functional Requirements: General		
ID	**Name**	**Description**
FR-1.10	Mobile-based Approvals	The ITSM Tool must include functionality that allows SSC and non-SSC GC employees the ability to approve or reject any type of ITSM-related approval request from a mobile device, including BlackBerry devices.
FR-1.11	Change & Release Calendar	The ITSM Tool must include an integrated change and release calendar that automatically displays the change and release activities recorded in the Tool.
FR-1.12	Multi-Tenancy	The ITSM Tool must support multi-tenancy, and the following use cases at a minimum, and through configuration: - The default state for multi-tenancy must be that tenants are unable to view or access the data of other tenants. - Each Tenant must be able to configure the ITSM processes independently of one another. This includes, but is not limited to: o ITSM record categories o SLA targets o Resolver Groups, Employees, Locations o Workflows, including Service Request models, Approvals and ticket routing - The ITSM Tool must allow SSC to configure specific SSC infrastructure assets (CIs) that can be viewed by a defined set of users in Customer Departments. - The ITSM Tool must allow SSC to configure specific Customer infrastructure assets (CIs) that can be viewed by a defined set of users at SSC. - The ITSM Tool must allow incidents assigned to a resolver group in one tenant to be assigned to a resolver group in another specific tenant. - The ITSM Tool must allow GC Customer tenants to have visibility of upcoming Change Management activity planned by SSC and vise-versa.
FR-1.13	Import/Export Functionality	The ITSM Tool must include a GUI-based method for importing and exporting data to and from the ITSM Tool, respectively. At a minimum, the ITSM Tool must support .XML and comma-delimited file formats for export and import.
FR-1.14	Queue Management	The ITSM Tool must include customizable screens, including functionality to allow users in different roles to manage and filter their work queues (Incidents, Change Requests, Service Requests, Etc.)
FR-1.15	Automatic Ticket Routing	The ITSM Tool must include functionality that allows process administrators to define rules and/or workflows to intelligently route ITSM tickets (E.g. Incidents, Change Requests, Service Requests) to the correct resolver group based on data attributes of the ticket.
FR-1.16	Impact	The ITSM Tool must include functionality that allows users to visualize impacted end-users/services from the Incident or Change Request screens.
FR-1.17	Process Flexibility	The ITSM Tool must be flexible in how ITSM processes are designed and configured. For example, it must be possible to add or remove one or more approval gates to a process, through configuration.
FR-1.18	User Notifications	The ITSM Tool must include functionality to send user notifications from the system in the user's chosen language.

2 SELF-SERVICE PORTAL (SSP)

Functional Requirements: Self-Service Portal (SSP)		
ID	**Name**	**Description**
FR-2.1	Portal for End Users	The ITSM Tool must include a self-service portal where end user may view the catalogue of services that they are entitled to, access knowledge base articles and FAQs, submit, update and monitor the status of their incidents and requests and view the status of relevant problems.
FR-2.2	Support for Business Line Services	The ITSM Tool must include functionality that allows customers/end-users to order goods and services from various non-IT lines of business (e.g. HR, Facilities).
FR-2.3	Search Capability	The ITSM Tool must include functionality that allows the end user to search knowledge base for solution via keyword, Boolean operators and full-text search.
FR-2.4	Align Content with End User Needs	The ITSM Tool must include functionality that allows for the association of end users with specific groups, lines of business, etc., and to tailor presented content, information and self-service options based on specific role or group entitlements.
FR-2.5	Survey Capability	The ITSM Tool must include functionality to create, deliver and manage end user satisfaction surveys (e.g. incident closure).
FR-2.6	Capture End User Feedback	The ITSM Tool must include functionality that allows administrators to provide a "suggestion box" for soliciting feedback from customers on process and interface.
FR-2.7	Chat Support	The ITSM Tool must have the capability to provide “chat” support for self-service usage.
FR-2.8	Bulletin Board Functionality	The ITSM Tool must include functionality to publish service related information including outages, scheduled downtimes and other issues.
FR-2.9	External Partner/Public Use	The ITSM Tool must include the ability to extend the use of the portal to external partners (e.g. provincial partners, airport authority, etc.) and Canadian public.

3 SERVICE CATALOGUE MANAGEMENT (SCM)

Functional Requirements: Service Catalogue Management (SCM)		
ID	**Name**	**Description**
FR-3.1	Different Service Types	The ITSM Tool must include functionality to have different types of services in the service catalogue, such as customer-facing services, technical service, supporting services.
FR-3.2	SCM User Access	The ITSM Tool must utilize role-based security to control access to the service catalogue.
FR-3.3	Organizing Services	The ITSM Tool must include functionality that allows services to be organized into logical groupings or hierarchical structures. This must be reflected in the self-service portal.
FR-3.4	Service Definition	The ITSM Tool must include functionality that provides configurable service definition templates out of the box.
FR-3.5	Service Entitlements	The ITSM Tool must include functionality that allows service catalogue managers to assign entitlements to service offering so that end users are only allowed to request offerings that they are entitled to. Entitlements

Functional Requirements: Service Catalogue Management (SCM)		
ID	**Name**	**Description**
		must be flexible in terms of how they are assigned (e.g. location, Org unit, etc.)
FR-3.6	Structured Content	The ITSM Tool must include functionality to publish services using a structured content framework for services, service offerings, etc. including descriptions, associated features, benefits, service levels, and pricing/costing.
FR-3.7	Service Level Assignment	The ITSM Tool must include functionality that allows SSC to support different service levels for the same service (e.g., bronze, silver, gold levels).
FR-3.8	Search Capability	The ITSM Tool must include functionality that allows users to quickly find services via a search engine.
FR-3.9	Request Service	The ITSM Tool must include functionality that allows users to create and track service requests through the service catalogue via the self-service portal.
FR-3.10	Multifunction Support	The ITSM Tool must include functionality that allows the service catalogue to support multiple business line (example: IT, HR, facilities, procurement).
FR-3.11	CMDB Integration	The ITSM Tool must include functionality for the service catalogue to integrate with the configuration management database and allow for the categorization of services and service CI information to be shared across the service catalogue and CMDB modules.
FR-3.12	Service Status	The ITSM Tool must include functionality to handle different service states (for example, services in design versus services in production).
FR-3.13	Business Line Support	The ITSM Tool must have the include functionality that allows business lines to create service definitions, design service workflow and easily publish these services into the catalogue.

4 PERFORMANCE REPORTING (PR)

Functional Requirements: Performance Reporting (PR)		
ID	**Name**	**Description**
FR-4.1	Construct Queries and Reports	The ITSM Tool must include functionality that allows users to easily construct queries and reports using attributes that span ITSM entities. (E.g. Change Requests and related tasks, CIs)
FR-4.2	Ad-hoc Reports	The ITSM Tool must include functionality that allows for the creation of custom ad-hoc parameters on reports (e.g., report is called and prompts user to enter query parameter values instead of hard-coding those values in the query). Individual users of all types require this ability.
FR-4.3	Standard Reports	The ITSM Tool must have predefined standard reports for users and administrators.
FR-4.4	Export Capability	The ITSM Tool must include functionality to easily export reports and report data for consumption outside the system. (i.e. PDF, xls).
FR-4.5	Report Drill Down Capability	The ITSM Tool must include functionality to "drill down" on reports and dashboards from within the ITSM software's UI
FR-4.6	External Data Integration	The ITSM Tool must have the capability to integrate with external data sources.

Functional Requirements: Performance Reporting (PR)		
ID	**Name**	**Description**
FR-4.7	Business Analytics	The ITSM Tool must have the capability to support business analytics (business intelligence tools).
FR-4.8	Restrict Access	The ITSM Tool must include functionality to restrict access to reports by role.
FR-4.9		*Intentionally left blank*
FR-4.10		*Intentionally left blank*
FR-4.11	Historical Reporting	The ITSM Tool must include functionality that allows selection field values to be removed, but preserved in the database for historical reporting purposes. This applies to drop-downs, menus, radio buttons, check boxes etc.
FR-4.12	Dashboard Capability	The ITSM Tool must include functionality for real-time reporting via graphical and configurable dashboards.
FR-4.13	Dashboard Display	The ITSM Tool must include functionality that provides real-time dashboard display for each process that is customizable based on individual, role or informational needs.
FR-4.14	Trending Reports	The ITSM Tool must include functionality that provides historical trending reports and volumetics specific to each ITSM process. (Incident Management, Request Fulfillment, Problem Management, Change Management, Service Catalogue Management, etc.).

5 INCIDENT MANAGEMENT (IM)

Functional Requirements: Incident Management (IM)		
ID	**Name**	**Description**
FR-5.1	Incidents and Service Requests	The ITSM Tool must store incidents and requests separately, as different record types.
FR-5.2	Incident Records	The ITSM Tool must include functionality that allows users to create, classify, update and close or cancel incident records.
FR-5.3	Incident Record Creation	The ITSM Tool must enforce required fields to be populated, and that all fields are populated with the intended data type and format as incident records are created and modified.
FR-5.4	Ticket Initiation	The ITSM Tool must include functionality that allows users to initiate a ticket on behalf of someone else, and store both the requestor and author of the incident.
FR-5.5	Link Incidents to Other Records	The ITSM Tool must include functionality that allows users to link incidents to problems, knowledgebase, known workarounds and change records.
FR-5.6	Link Incidents to Services/CIs	The ITSM Tool must include functionality that allows users to link incident records to the impacted service(s), CIs and group of CIs.
FR-5.7	Link to Multi-Service Tiers	The ITSM Tool must include functionality that allows users to manage and link incident records to multiple tiers of service/service levels depending on customer and associated service.
FR-5.8	View Impacted CIs	The ITSM Tool must include functionality that allows users to view impacted CIs from within an incident record, and to view upstream and downstream affected CIs and services through a visual depiction.

Functional Requirements: Incident Management (IM)		
ID	**Name**	**Description**
FR-5.9	Incident Categorization	The ITSM Tool must include functionality that allows users to categorize incidents based on a standard categorization scheme.
FR-5.10	Incident Prioritization	The ITSM Tool must include functionality that allows users to prioritize incidents based on a standard prioritization scheme that is derived through assessment of business impact and business urgency.
FR-5.11	Incident Matching	The ITSM Tool must include functionality that allows users to match incidents to determine if an incident is a duplicate or if it might be related to an existing problem or known error.
FR-5.12	Incident Automation	The ITSM Tool must include functionality to automate incident models (e.g. chronological order and dependencies of steps to be actioned by specific roles, timescales and thresholds for completion and required escalation) based on incident classification.
FR-5.13	Incident Routing	The ITSM Tool must include functionality to route incidents based on available resources located across multiple sites and other factors, such as time of day, tiered service values, incident classification, etc.
FR-5.14	Alert Capability	The ITSM Tool must include functionality to send incident management notifications using a variety of methods including e-mail, mobile device notification, pager or SMS text messaging.
FR-5.15	Escalation Capability	The ITSM Tool must include functionality for hierarchical escalation, both manually and automated based on business rules, upon incident status change, priority change and/or service level clock expiration.
FR-5.16	Information Capture	The ITSM Tool must include functionality that allows users to input free text, screen captures, and file attachments while recording incident descriptions and resolution activities.
FR-5.17	Time Stamping	The ITSM Tool must include functionality that allows users to track the time that an incident was in a specific status during its lifecycle (e.g. initial diagnosis, investigation, resolved), and how long an incident was assigned to each resolver group in the case of reassignment. This information must be available in the software's UI and via reports.
FR-5.18	Knowledge Access	The ITSM Tool must include functionality that allows users to access knowledge and/or support scripts for incident diagnosis and resolution.
FR-5.19	Multiple Sequential Assignments	The ITSM Tool must include functionality to manage and maintain multiple sequential assignments for each open Incident.
FR-5.20	Collaboration	The ITSM Tool must include functionality that allows members of multiple resolver groups to collaborate on a single incident
FR-5.21	Hierarchical Escalation Notification	The ITSM Tool must include functionality for hierarchical notification about incidents that exceed or will soon exceed priority/service level parameters.
FR-5.22	Hold Status	The ITSM Tool must include functionality that allows users to put incidents on hold in certain (configurable) situations so time does not count against service level targets.
FR-5.23	View Time Left	The ITSM Tool must include functionality that allows users to see countdown time left on response or resolve time (associated with priority or service level targets)
FR-5.24	User Notification	The ITSM Tool must include functionality to trigger a notification to the user when a ticket is placed in a resolved status.

Functional Requirements: Incident Management (IM)		
ID	**Name**	**Description**
FR-5.25	Automated Ticket Closure	The ITSM Tool must include functionality to automatically close tickets at a predetermined number of business days after a ticket enters resolved status.
FR-5.26	Closure Codes	The ITSM Tool must include functionality to use configurable closure categorization codes upon incident closure.
FR-5.27	Survey Capability	The ITSM Tool include functionality to collect end-user satisfaction feedback upon the close of an incident.
FR-5.28	Incident Reactivation	The ITSM Tool must include functionality that allows users to reactivate incident in resolved status.
FR-5.29	Event/Incident Integration	The ITSM Tool must have the capability to automatically create, update and close incidents upon receiving information from an integrated event monitoring tool.
FR-5.30	Self-Service Portal Integration	The ITSM Tool must include functionality that allows users to submit incidents and view their status via a self-service portal.
FR-5.31	Email Support	The ITSM Tool must include functionality that allows users to submit incidents via email and also receive timely updates, through email system integration.
FR-5.32	Change/Problem Creation	The ITSM Tool must include functionality that allows users to create a change or problem from an incident with automatic population of fields.
FR-5.33	Problem Management Integration	The ITSM Tool must include integration with Problem Management allowing for viewing of problem and known error details for the use in matching, troubleshooting and resolution and linking incident records to related problem records.
FR-5.34	Change Management Integration	The ITSM Tool must include integration with Change Management allowing for the creation of a change record to resolve an incident and to link associated incident record(s) to the change record.
FR-5.35	Service Asset and Configuration Management	The ITSM Tool must include integration with Service Asset and Configuration Management allowing for the linking of incident records to CI records in order to make CI information available to assist in the classification and prioritization of incidents and allow visibility into incidents associated with a CI or set of CIs.
FR-5.36	Knowledge Management Integration	The ITSM Tool must include integration with Knowledge Management allowing for access to knowledge articles, support scripts, and known workarounds for incident diagnosis, creating knowledge entries and publishing end-user based FAQs.
FR-5.37	Service Level Management Integration	The ITSM Tool must include functionality to link to service levels for alerting and so that impact can be assessed if a service is performing below agreed upon levels.
FR-5.38	Recurring Incident Templates	The ITSM Tool must include functionality that allows users to develop templates for recurring incidents.

6 REQUEST FULFILLMENT (RFL)

Functional Requirements: Request Fulfillment (RFL)		
ID	**Name**	**Description**
FR-6.1	Service Request Records	The ITSM Tool must include functionality that allows users to create, classify, approve, update, and close or cancel service request records.
FR-6.2	Service Request Record Creation	The ITSM Tool must enforce required fields to be populated, and that all fields are populated with the intended data type and format as incident records are created and modified.
FR-6.3	Attachments	The ITSM Tool must include functionality that allows users to submit attachments as part of a service request and have them stored in the record.
FR-6.4	Request Models	The ITSM Tool must include functionality that allows users to configure dynamic request models and workflows for different types of requests that support multi-level approvals, answer-based decisions and paths, and a variety of fulfillment options (E.g. change request, orchestration)
FR-6.5	Workflow Capability	The ITSM Tool must include functionality that allows users to configure a service request workflow from initial request to fulfillment including: i. the ability to support serial and parallel workflow paths; and ii. the ability to identify and associate approval and information points required during the flow until final delivery is successfully accomplished.
FR-6.6	Authorized Requestors	The ITSM Tool must include functionality that limits viewing, creating and editing requests only to authorized requestors.
FR-6.7	Service Request Categorization	The ITSM Tool must include functionality that allows users to categorize service requests based on a standard categorization scheme.
FR-6.8	Service Request Prioritization	The ITSM Tool must include functionality that allows users to prioritize service requests based on a standard prioritization scheme that is derived from the assessment of business impact and business urgency.
FR-6.9	Request Automation	The ITSM Tool must include functionality to automatically send, receive and log approvals for requests.
FR-6.10	Automation Override	The ITSM Tool must include functionality that allows users to manually override automation, when required.
FR-6.11	Automatic Routing	The ITSM Tool must include functionality to automatically route requests for appropriate authorization and fulfillment.
FR-6.12	Task Assignment	The ITSM Tool must include functionality to assign tasks to groups or individuals to be accomplished within a specified time frame. The ITSM Tool software must notify the assignee of the task and due date.
FR-6.13	Time Tracking	The ITSM Tool must include functionality that allows users to track the time that a service request was in a specific status during its lifecycle (e.g. received, assigned, being fulfilled, complete, closed), and how long a request was assigned to each resolver group in the case of reassignment. This information must be available in the software's UI and via reports.
FR-6.14	Service Level Targets	The ITSM Tool must include functionality that allows users to see countdown time left on fulfillment time (associated with service level targets) and trigger automated escalation if target is breached.

Functional Requirements: Request Fulfillment (RFL)		
ID	**Name**	**Description**
FR-6.15	Automated Status Updates	The ITSM Tool must include functionality to provide automated status updates to requestors when a request reaches specific points in the workflow.
FR-6.16	Request Cancellation	The ITSM Tool must include functionality that allows users to cancel a service request through the self-service portal.
FR-6.17	Service Catalogue and Self-Service Portal Integration	The ITSM Tool must include integration with the service catalogue and self-service portal, allowing users view and request services through the portal based on their entitlement.
FR-6.18	Service Asset and Configuration Management Integration	The ITSM Tool must include integration with Service Asset and Configuration Management allowing for the linking of service request records to CI records.
FR-6.19	Change Management Integration	The ITSM Tool must include integration with Change Management allowing for the creation of a change record where required to fulfill a request.
FR-6.20	Integration with Other Fulfillment Technologies	The ITSM Tool must have the capability to integrate with other fulfillment technologies (e.g. VM provisioning, orchestration), which will update the request to indicate when fulfillment is completed.

7 CHANGE MANAGEMENT (CHGM)

Functional Requirements: Change Management (CHGM)		
ID	**Name**	**Description**
FR-7.1	Change Records	The ITSM Tool must include functionality that allows users to create, classify, approve, update and close or cancel change records.
FR-7.2	Change Record Creation	The ITSM Tool must include functionality that allows authorized users to create new change records, enforce data rules and types, and required fields.
FR-7.3	Link Changes to Services/CIs	The ITSM Tool must include functionality that allows users to link change records to impacted service(s), CIs, and group of CIs.
FR7.4	View Impacted CIs	The ITSM Tool must include functionality that allows users to view impacted CIs from within a change record, and to view upstream and downstream affected CIs and services through a visual depiction.
FR-7.5	Change Categorization	The ITSM Tool must include functionality that allows users to categorize changes based on a standard categorization scheme.
FR-7.6	Change Prioritization	The ITSM Tool must include functionality that allows users to prioritize changes based on a standard prioritization scheme that is derived from the assessment of business impact and business urgency.
FR-7.7	Configure Risk Assessment	The ITSM Tool must include functionality that allows users to configure the parameters upon which risk is calculated by the Tool considering business impact, affected application/business services criticality, collision, historical

Functional Requirements: Change Management (CHGM)		
ID	**Name**	**Description**
		change information, and compliance with maintenance windows and black-out periods.
FR-7.8	Risk and Impact Analysis	The ITSM Tool must include functionality to automatically determine risk and impact analysis of multiple changes, and provide visual depictions of upstream and downstream CIs that can be navigated based on information in a configuration management database (CMDB).
FR-7.9	Information Capture	The ITSM Tool must include functionality that allows users to enter free form text, screen captures, and file attachments for recording of change request descriptions.
FR-7.10	Templated Change Workflow	The ITSM Tool must provide templated workflow for pre-approved, normal and emergency change types, including pre-defined classification field values as well as tasks involved in the specific type of change.
FR-7.11	Tasks	The ITSM Tool must include functionality to: i. Sequence and re-sequence tasks; ii. Group tasks; and iii. Allow tasks to be completed in serial or parallel
FR-7.12	Task Assignment	The ITSM Tool must include functionality that allows users to assign tasks to groups or individuals to be accomplished within a specified time frame. The Tool shall notify the assignee of the task and due date.
FR-7.13	Documentation	The ITSM Tool must include functionality that allows users to store back-out procedures, installation and turnover documents within the change record.
FR-7.14	CAB Support	The ITSM Tool must include functionality to support a CAB (i.e., approvals/issues submitted and stored electronically).
FR-7.15	Role-based Approval	The ITSM Tool must include functionality to have multiple role-based approvers and electronic routing of those approvals.
FR-7.16	Automated Approval Workflow	The ITSM Tool must provide Automated Approval workflow functionality including: i. Ability to automatically send approval requests to designated approvers based at a minimum on categorization, impact, risk level, location, impacted CIs, areas, or customers, etc.). ii. Ability to pick up and record approver responses. iii. Ability to change status if approval criteria met. iv. Send notification of approval (rejection) to change owner and change manager.
FR-7.17	Approval Request Capability	The ITSM Tool must include functionality to: i. send approval requests several times (manually or automatically based on record conditions); ii. store multiple instances of approvals; iii. reset approval status; iv. resend approval requests (manually or automatically based on record conditions); and v. record the history and results of request approvals.
FR-7.18	Repeatable Changes	The ITSM Tool must include functionality that allows users to select and create change requests from a viewable library and select an associated predefined template with prepopulated content, such as categorization, text, tasks and CIs.
FR-7.19	Proactive Notification	The ITSM Tool must include functionality to provide proactive notification to stakeholders and change advisory board (CAB) members for changes with significant business impact, collisions and compliancy issues.

Functional Requirements: Change Management (CHGM)		
ID	**Name**	**Description**
FR-7.20	Change Calendar	The ITSM Tool must include a change calendar with scheduled change viewing by group, and to customize the sorting and filtering of calendar views.
FR-7.21	Change Scheduling	The ITSM Tool must include functionality that allows users to schedule recurring events, such as certain types of maintenance.
FR-7.22	Microsoft Exchange Integration	The ITSM Tool must have the capability to integrate forward schedule of changes (FSC) with Microsoft Exchange calendaring system.
FR-7.23	Change Calendar (Cross Platform)	The ITSM Tool must automatically make the change calendar available across multiple platforms: (Mobile Device, web browser). The software must be able to publish or expose the change calendar to an external web page that is not part of the ITSM software.
FR-7.24	Support Freeze Windows	The ITSM Tool include functionality that allows users to define and enforce maintenance, release and moratoriums for freeze windows.
FR-7.25	Promote to a Release	The ITSM Tool must include functionality that allows users to promote one or more changes to a release within the application, and generate corresponding notifications to change and release stakeholders
FR-7.26	Change Notification	The ITSM Tool must include functionality to send an automated notification of changes to appropriate person(s) when change is updated, status change, etc.
FR-7.27	Change Dashboard	The ITSM Tool must include a change dashboard that can be customized by individual users based on person, group, service and customer.
FR-7.28	Automated Notifications (Start Time)	The ITSM Tool must include functionality to send automated notifications at the scheduled start time to all identified activity assignees to remind them of the change.
FR-7.29	Automated Notifications (Implementation)	The ITSM Tool must include functionality to send automated notifications upon individual change task completion, and overall change implementation completion.
FR-7.30	Link to Projects	The ITSM Tool must include functionality that allows users to link change records to projects.
FR-7.31	Status Tracking	The ITSM Tool must include functionality that allows users to review the status of change requests including who updated the status at what date/time. This includes past history.
FR-7.32	Automatic Warnings	The ITSM Tool must include functionality to automatically warn the user of any changes that exceed pre-specified time periods during any stage.
FR-7.33	Automatic Warnings	The ITSM Tool must include functionality to warn users if the change request they are planning impacts or changes infrastructure or services being impacted or changed by other change requests in the same timeframe.
FR-7.34	Incident Management Integration	The ITSM Tool must include integration with Incident Management allowing for the linking of incident records to change records in order to provide full visibility of incidents caused by changes.
FR-7.35	Request Fulfillment Integration	The ITSM Tool must include integration with Request Fulfillment allowing for the creation of a change record where required to fulfill a request.

Functional Requirements: Change Management (CHGM)		
ID	**Name**	**Description**
FR-7.36	Problem Management Integration	The ITSM Tool must include integration with Problem Management allowing for the linking of problem records to change records in order to provide full visibility into problems caused by changes.
FR-7.37	Service Asset and Configuration Management Integration	The ITSM Tool must include integration with Service Asset and Configuration Management allowing for the linking of change records to CI records and to make up-to-date CI information readily available to assist in prioritizing and assessing the impact of changes.
FR-7.38	Release and Deployment Management Integration	The ITSM Tool must include integration with Release and Deployment Management allowing for the linking of change records to release records and to view the status of releases.
FR-7.39	Service Catalogue and Service Portal Interface	The ITSM Tool must include integration with the service catalogue and self-service portal, allowing specific user types to view and request services through the portal based on their entitlement.
FR-7.40	Service Level Management Integration	The ITSM Tool must include functionality to link to service levels for alerting and so that impact can be assessed if a change is performing below agreed upon levels.
FR-7.41	Time Tracking	The ITSM Tool must include functionality that allows users to track the time that a change request was in a specific status during its lifecycle (e.g. draft, planning, approval states, in progress), and how long a change request was assigned to each resolver group in the case of reassignment. This information must be available in the software's UI and via reports.

8 SERVICE ASSET AND CONFIGURATION MANAGEMENT (SACM)

Functional Requirements: Service Asset and Configuration Management (SACM)		
ID	**Name**	**Description**
FR-8.1	Access Control	The ITSM Tool must provide different levels of access to configuration information based on roles defined and assigned within the Tool.
FR-8.2	Add or Remove CI Types	The ITSM Tool must provide a data model and functionality that allows for the addition or removal of configuration item (CI) types and their corresponding fields. (Note: no programming skills or System Administrator permissions shall be required to add a CI type or its corresponding fields).
FR-8.3	Display CI Fields	The ITSM Tool must include functionality that allows users to display CI fields based on a CI type.
FR-8.4	Create New CIs	The ITSM Tool must include functionality that allows designated users to create new CIs (including fill in all field values).
FR-8.5	Data Validation Rules	The ITSM Tool must include functionality to enforce data validation rules on field values on creation of any new CI.
FR-8.6	Edit CI Field Values	The ITSM Tool must include functionality to edit any existing CI field values by varying degrees by authorized users.
FR-8.7	CI Dependencies	The ITSM Tool must include functionality to define the dependency relationship between CIs in both directions using custom terminology (i.e. hosted on, hosts).

Functional Requirements: Service Asset and Configuration Management (SACM)		
ID	**Name**	**Description**
FR-8.8	Graphical View of Dependencies	The ITSM Tool must include functionality to provide a graphical representation of the dependencies between CIs
FR-8.9	Automated Alerts	The ITSM Tool must include functionality to determine when a CI is in an authorized state (e.g. as a result of discovery and automated reconciliation) and automatically initiate a workflow action, or a role-based notification (E.g. CI owner)
FR-8.10	Assign Maintenance Windows	The ITSM Tool must include functionality that allows users to assign maintenance windows to any CIs.
FR-8.11	Freeze CIs	The ITSM Tool must include functionality to "freeze" a CI so that it cannot have a change logged against it.
FR-8.12	Auto Discovery	The ITSM Tool must have the capability to integrate with SSC's existing discovery tool (Tivoli Application Dependency Discovery Manager) and other industry best-of-breed discovery tools. The integration must support CI creation and updates, as well as the creation and maintenance of dependency relationships between CIs if these have been modelled in the discovery tool.
FR-8.13	Reconciliation	The ITSM Tool must include functionality to reconcile discovered CIs against those CIs already in the CMDB so that only the correct attributes on the correct CI(s) are updated. The Tool must possess configuration-based means to ensure that discovered CIs are populated in the CMDB with valid data (classification, product catalog references, etc.). This process must occur on a scheduled or continuous basis and be configurable by business users with the appropriate level of access.
FR-8.14	Multiple Data Sources	The ITSM Tool Solution must be able to receive CI and relationship data from a variety of sources and configure the reconciliation rules differently for each.
FR-8.15	Set Workflow Triggers	The ITSM Tool must include functionality to set automatic workflow triggers based on CI attribute values (e.g. change of CI status).
FR-8.16	Audit Trail of Changes (Attributes)	The ITSM Tool must include functionality to maintain an audit trail of changes made to a CI attribute over time.
FR-8.17	Audit Trail of Changes (CI)	The ITSM Tool must include functionality to maintain an audit trail of change requests made to a CI over time.
FR-8.18	Search Capability	The ITSM Tool must include functionality that allows users to search for a CI by any CI field, or combination of fields.
FR-8.19	Ad Hoc Queries	The ITSM Tool must include functionality that allows users to perform ad hoc/general queries.
FR-8.20	Data Import / Export	The ITSM Tool must include functionality that supports both flexible data import/export including: - Flexible file types (XML, csv) - Scheduled/Automated import jobs
FR-8.21	Incident Management Integration	The ITSM Tool must include integration with Incident Management allowing for the linking of incident records to CI records and to make CI information readily available to assist in the classification and prioritization of incidents.

Functional Requirements: Service Asset and Configuration Management (SACM)		
ID	**Name**	**Description**
FR-8.22	Problem Management Integration	The ITSM Tool must include integration with Problem Management allowing for the linking of problem records to CI records and to make CI information readily available to assist in the classification and prioritization of problems.
FR-8.23	Change Management Integration	The ITSM Tool must include integration with Change Management allowing for the linking of change records to CI records and to make CI information readily available to assist in prioritizing and assessing the impact of changes.
FR-8.24	Release Management Integration	The ITSM Tool must include integration with Release Management allowing for the display and reporting of impacted CIs via their link to changes associated with a release.
FR-8.25	Service Level Management Integration	The ITSM Tool must include integration with Service Level Management allowing for the linking of services to CI records and to make CI information readily available to assist in determining service dependencies.
FR-8.26	Request Fulfillment Integration	The ITSM Tool must include integration with Request Fulfillment allowing for the linking of service requests to CI records.
FR-8.27	Service Catalogue Integration	The ITSM Tool must include integration with Service Catalogue allowing for the linking of services to CI records and to make CI information readily available to assist in determining service dependencies.
FR-8.28	Knowledge Management Integration	The ITSM Tool must include integration with Knowledge Management allowing for the linking of knowledge to CI records.
FR-8.29	Asset Tracking	The ITSM Tool must include functionality that allows users to track asset status and lifecycle management such as procurement, stored, configured, deployed, active, retired and disposed stages to support release impact analysis, planning, rollout and deployment activities.
FR-8.30	Release Support	The ITSM Tool must include functionality to support release impact analysis, planning, rollout and deployment activities.
FR-8.31	Contracts and Licensing Agreements	The ITSM Tool must include functionality that allows users to record a wide variety of contracts and licensing agreements by attaching them to records.
FR-8.32	Contract and Agreement Tracking	The ITSM Tool must include functionality that allows users to track the physical location of contracts and agreements, and identify the individuals responsible for them.
FR-8.33	Software Audit	The ITSM Tool must have the capability for Multiple Software Audit options – import software audit information from FrontRange Discovery, Microsoft SMS & SCCM and other solutions.
FR-8.34	Software Licencing Models	The ITSM Tool must include functionality to support Multiple Licensing Models for tracking software – from off-the-shelf application through to company-wide and version maintenance agreements.
FR-8.35	Software License Management	The ITSM Tool must include functionality to perform software license management including automated notification of license expiration and non-compliance and reporting, tracking and auditing
FR-8.36	Costing Support	The ITSM Tool must include functionality that allows for the grouping of an individual customer's/user's assets/CIs and services to provide cost information.
FR-8.37	Lease, Warranty and Contract Management	The ITSM Tool must include functionality that allows users to manage leases, depreciation schedules, warranties, and service provider contracts.

Functional Requirements: Service Asset and Configuration Management (SACM)		
ID	**Name**	**Description**
FR-8.38	Track Asset/ CI Costs	The ITSM Tool must include functionality that allows users to track both fixed and variable costs of assets/CIs.
FR-8.39	Barcode Scanners	The ITSM Tool must have the capability to interface with barcode scanning hardware and software for the purposes creating or updating CIs based on Asset Tag or Serial Number information.

9 SERVICE LEVEL MANAGEMENT (SLM)

Functional Requirements: Service Level Management (SLM)		
ID	**Name**	**Description**
FR-9.1	Agreements and Contracts	The ITSM Tool must include functionality that allows users to store agreements and contracts.
FR-9.2	Store SLM information in CMDB	The ITSM Tool must include functionality that allows users to store Service Level Management information (service levels, agreements, contracts, reports) in CMDB as structured data.
FR-9.3	Multiple SLA Structure Support	The ITSM Tool must include functionality to support multiple SLA structures and store information related to master agreements, extensions and/or addendums for specific business units.
FR-9.4	Service Level Performance	The ITSM Tool must include functionality to link service levels to business units or departments, so that impact can be assessed if a service is performing below agreed upon levels.
FR-9.5	Historical Service Information	The ITSM Tool must include functionality to retain and maintain historical data and information on services. This includes service level result data for each service.
FR-9.6	Multiple Service Level Targets	The ITSM Tool must have the capability to allow process administrators to configure multiple service level targets for each process. (E.g. An incident may have targets for response and resolution). Each target must be able to have multiple time thresholds that can trigger different escalation actions (E.g. notify different stakeholders at 30, 15 and 5 minutes before target is breached)
FR-9.7	Service Dashboards	The ITSM Tool must include functionality that allows users to create dashboards or scorecards that communicate service performance to Service Owners/Leads and other interested parties.
FR-9.8	Management of Service Level Targets	The ITSM Tool must include functionality to automate the management of service level targets in terms of automated business rules, alerts, escalations and notifications.
FR-9.9	Support Levels	The ITSM Tool must include functionality that allows users to publish different service levels for the same service.
FR-9.10	Search Engine	The ITSM Tool must include functionality of a search engine to facilitate locating service information.
FR-9.11	Multiple Contracts	The ITSM Tool must include functionality that allows users to define multiple contract types and contracts per customer.
FR-9.12	Priority Definitions and Action Times	The ITSM Tool must include functionality to handle different priority definitions and action times for each customer.
FR-9.13	Agreement and Contract Review	The ITSM Tool must include functionality that allows users to schedule agreement and contract review cycles and renewals.

Functional Requirements: Service Level Management (SLM)		
ID	**Name**	**Description**
FR-9.14	Service Level Achievement Against Target	The ITSM Tool must include functionality that allows users to report on service level achievements vs. service level targets in real-time and at regular planned intervals.

10 EVENT MANAGEMENT (EM)

Functional Requirements: Event Management (EM)		
ID	**Name**	**Description**
FR-10.1	Event Monitoring and Incident Management Integration	The ITSM Tool must have the capability to integrate event and alert monitoring tools with Incident Management to allow for automatic creation and update of incidents from these tools, based on business rules.
FR-10.2	Service Impact Assessment	The ITSM Tool must include functionality that allows users to identify which customer-facing service(s) is impacted by an event based on service/CI dependency mapping (CMDB), when an incident is created either manually or through the integration with an event and/or alert monitoring tool.

11 KNOWLEDGE MANAGEMENT (KM)

Functional Requirements: Knowledge Management (KM)		
ID	**Name**	**Description**
FR-11.1	Search Capability	The ITSM Tool must include functionality that allows users to launch fast knowledge searches from other ITSM record types (e.g. Incident) using the categorization (or partial categorization) selections as key value search parameters.
FR-11.2	Search Capability	The ITSM Tool must include functionality that provides knowledge management capabilities by displaying the most relevant hits at the top, in order of closest match to search.
FR-11.3	Weighting and Scoring Articles	The ITSM Tool must include functionality that allows a knowledge manager to administer the weighting and relevancy scores associated with knowledge articles (e.g. based on key word searching and usage).
FR-11.4	Article Creation	The ITSM Tool must include functionality that allows users to create a knowledge article via a fill-in-the-blank template.
FR-11.5	Role-based Knowledge	The ITSM Tool must support role-based knowledge items, in terms of which roles can access various types of articles. (i.e., a technical role can access either technical-facing or customer-facing articles).
FR-11.6	Create KM Entries from other Modules	The ITSM Tool must include functionality that allows users to create knowledge management entries from incident, problem, request fulfillment and change modules.
FR-11.7	Article Lifecycle Management	The ITSM Tool must include functionality to manage full life cycle of knowledge articles through administration capabilities (e.g., submission, editing, review, approval, publishing, usage monitoring, etc.).
FR-11.8		*Intentionally left blank*
FR-11.9	Rich-text Editor	The ITSM Tool must provide a rich-text editor (RTE) that supports links within documents, document-to-document links and attaching images to documents.
FR-11.10	Automated Administration	The ITSM Tool must provide automated administration capabilities, including ease of adding, editing and maintaining the data, and ability for end-user submission to require review/approval prior to posting.
FR-11.11	Graphical Workflow	The ITSM Tool must include functionality that allows users to define workflow process for reviewing and approving pending knowledge articles that can be displayed graphically.
FR-11.12	Mandatory Template Fields	The ITSM Tool include functionality that allows authorized users to make certain fields in the knowledge article template mandatory.
FR-11.13	Embed Web Links, Images and Objects	The ITSM Tool must include functionality that allows users to embed Web links, images and objects into knowledge articles (e.g., screenshots, etc.).
FR-11.14	Search Capability	The ITSM Tool must include functionality that allows users to search across all sections of a knowledge article from a single search field.
FR-11.15	Feedback Mechanism	The ITSM Tool must include functionality that allows users to provide feedback to rate/score content for usefulness related to the inquiry.
FR-11.16	Knowledge-Centered Support	The ITSM Tool must be able to provide knowledge-centered support (KCS) standards and guidelines based Knowledge Management system.

12 PROBLEM MANAGEMENT (PM)

Functional Requirements: Problem Management (PM)		
ID	**Name**	**Description**
FR-12.1	Problem Records	The ITSM Tool must include functionality that allows users to create, update, and close or cancel problem records.
FR-12.2	Problem Record Creation	The ITSM Tool must enforce required fields to be populated, and that all fields are populated with the intended data type and format as incident records are created and modified.
FR-12.3	Information Capture	The ITSM Tool must include functionality that allows users to enter free text, screen captures, and file attachments for the recording of problem descriptions and resolution activities.
FR-12.4	View Impacted CIs	The ITSM Tool must include functionality that allows users to view impacted CIs from within a problem record, and to view upstream and downstream affected CIs and services through a visual depiction.
FR-12.5	Time Tracking	The ITSM Tool must include functionality that allows users to track the time that a problem was in a specific status during its lifecycle (e.g. initial diagnosis, investigation, resolved), and how long a problem was assigned to each resolver group in the case of reassignment. This information must be available in the software's UI and via reports.
FR-12.6	Link Problems to Services/CIs	The ITSM Tool must include functionality that allows users to link problems/known error records to a service(s), CIs, and group of CIs.
FR-12.7	Problem Categorization	The ITSM Tool must include functionality that allows users to categorize changes based on a standard categorization scheme.
FR-12.8	Problem Prioritization	The ITSM Tool must include functionality that allows users to prioritize changes based on a standard prioritization scheme that is derived from the assessment of business impact and business urgency.
FR-12.9	Problem / Known Error Differentiation	The ITSM Tool must include functionality that allows users to differentiate between problems and known errors.
FR-12.10	Task Assignment	The ITSM Tool must include functionality that allows users to assign tasks to groups or individuals to be accomplished within a specified time frame. The ITSM Tool software must notify the assignee of the task and due date and the associated problem record.
FR-12.11	Cause Codes	The ITSM Tool must include functionality that allows users to use configurable cause codes as input to categorizing a problem.
FR-12.12	Closure Codes	The ITSM Tool must include functionality that allows users to use configurable closure categorization codes upon problem closure.
FR-12.13	Self-Service Portal Integration	The ITSM Tool software must include integration with the self-service portal, allowing users to view problems and their status.
FR-12.14	Incident Management Integration	The ITSM Tool must include integration with Incident Management allowing for the linking of incident records to problem records in order to provide full visibility into incidents caused by problems and the impact of problems on the business users.
FR-12.15	Change Management Integration	The ITSM Tool must include integration with Change Management allowing for the creation of a change record to resolve a problem and to view changes that may provide input to resolve problems.

Functional Requirements: Problem Management (PM)		
ID	**Name**	**Description**
FR-12.16	Service Asset and Configuration Management Integration	The ITSM Tool must include integration with Service Asset and Configuration Management allowing for the linking of problem records to CI records in order to make CI information readily available to assist in the classification and prioritization of problems and to allow visibility into problems associated with a CI or set of CIs.
FR-12.17	Knowledge Management Integration	The ITSM Tool must include integration with Knowledge Management allowing for the documenting and managing of knowledge articles pertaining to a problem and publishing of end-user based FAQ's and supporting reference documents within the knowledgebase.
FR-12.18	Knowledge Base Reporting	The ITSM Tool must include functionality that allows users to report on the number of proposed solutions, most used solutions, and least used solutions in the knowledgebase.

13 RELEASE AND DEPLOYMENT MANAGEMENT (RDM)

Functional Requirements: Release and Deployment Management (RDM)		
ID	**Name**	**Description**
FR-13.1	Release Records	The ITSM Tool must include functionality that allows users to create, update, and close or cancel release records.
FR-13.2	Related Changes	The ITSM Tool must include functionality that allows users to log a release so that changes can be identified and related to the release.
FR-13.3	Release Record Capture	The ITSM Tool must include functionality that allows users to capture the release date and time, identify who will be implementing and link resources to the release.
FR-13.4	Attach Documents	The ITSM Tool must include functionality that allows users to attach and store documentation with the release record.
FR-13.5	View Impacted CIs	The ITSM Tool must include functionality that allows users to view impacted CIs through the related change records.
FR-13.6	Task Assignment	The ITSM Tool must include functionality that allows users to assign tasks to groups or individuals to be accomplished within a specified time frame. The ITSM Tool software must notify the assignee of the task and due date.
FR-13.7	Change Status	The ITSM Tool must include functionality that allows users to change status of release and linked changes, release documentation and release approvals.
FR-13.8	Change Status Notification	The ITSM Tool must include functionality to automatically notify the release coordinator when the status of a change associated with a release changes status.
FR-13.9	Search Capability	The ITSM Tool must include functionality that allows users to search all releases by any release data attribute captured by the Tool.
FR-13.10	Release Windows	The ITSM Tool must include functionality that allows users to define release windows (show conflicts that impact when releases can be scheduled).
FR-13.11	Master Release Schedule	The ITSM Tool must include functionality that allows users to create and publish a Master Release Schedule.
FR-13.12	Problem Management Integration	The ITSM Tool must include integration with Problem Management allowing for the linking of problem and known error records to release records.

Functional Requirements: Release and Deployment Management (RDM)		
ID	**Name**	**Description**
FR-13.13	Change Management Integration	The ITSM Tool must include integration with Change Management allowing for the linking of release records to change records.
FR-13.14	Service Asset and Configuration Management Integration	The ITSM Tool must include integration with the CMDB to support the association of release records to CI records.
FR-13.15	CMDB Support	The ITSM Tool must be able to validate required information from the CMDB for release build and deployment activities.
FR-13.16	Release Readiness	The ITSM Tool must support the establishment and governance of release readiness criteria.
FR-13.17	Authorization Support	The ITSM Tool must include functionality that allows users to authorize and schedule release deployments in conjunction with the Change Management process.
FR-13.18	Post Deployment	The ITSM Tool must include functionality that allows users to trace and track post deployment activities (e.g. early life support).

APPENDIX 3 – DEFINITIONS & ACRONYMS

Term or Acronym	Definition
ITSM Tool (or Tool)	Refers to the enterprise class ITSM Tool commercial off the shelf (COTS) software to be provided by the Contractor to meet the Non-Functional and Functional Requirements set out in Appendix 1 and 2 respectively.
ITSM Tool Solution	Refers to the overall solution to be provided by the Contractor, including but not limited to: provision of an ITSM Tool (software); System Integration (SI) professional services required to implement the new Tool; and Application Management Services (AMS).
ITSM Tool Contractor (or Contractor)	The corporate entity that is responsible for all goods and services (i.e. the Work) delivered under this Contract.
Enterprise ITSM Tool Project	Refers to the SSC initiative undertaken to select and implement a new enterprise class ITSM Tool software.
ITSM Toolset	Refers to the ITSM related software products currently in use at SSC.
Configuration	Configuration of the ITSM Tool, the resulting feature, business rule or workflow is limited to the following actions: a) Must be configured using screens or files that are documented in the software manufacturer's manuals. This may include: a. Filling out a form in an administration GUI in the ITSM Tool. b. Clicking a button or a link c. Changing a documented setting in a configuration file d. Running a wizard b) Must not require coding or knowledge of any industry or proprietary coding or scripting language. c) Must not involve modifications or overlays of objects or components originally shipped with the product. d) Must be supported by the Software Publisher's standard Maintenance and Support Services for the Licensed Software. e) Must be recognised by the Software Publisher's commercially available upgrade installers. In other words, the configuration must not require any additional backup, reconciliation, regression testing or analysis when upgrading the ITSM software, than functionality originally

Term or Acronym	Definition
Release	A Release (also referred to as a “Release Package”) consists of a single Release Unit or a structured set of Release Units. A Release Unit is a set of new, changed and/or unchanged Configuration Items, which are tested and introduced into the production environment together to implement one or several approved Changes. A release can therefore include hardware and software, documentation, processes, or other components that are essential to successfully implementing an approved change to the ITSM Tool Solution.
Agile	In software application development, agile software development (ASD) is a methodology for the creative process that anticipates the need for flexibility and applies a level of pragmatism into the delivery of the finished product. Agile software development focuses on keeping code simple, testing often, and delivering functional bits of the application as soon as they're ready. The goal of ASD is to build upon small client-approved parts as the project progresses, as opposed to delivering one large application at the end of the project.
Scrum	Scrum is a methodology that allows a team to self-organize and make changes quickly, in accordance with Agile principles.
Scrum Master	A scrum master is the facilitator for an Agile development team. The scrum master manages the process for how information is exchanged. The scrum master is responsible for removing any impediments to progress, facilitating meetings, and doing things like working with the product owner to make sure the product backlog is in good shape and ready for the next sprint.
Sprint	In product development, a **sprint** is a set period of time during which specific work has to be completed and made ready for review. Each **sprint** begins with a planning meeting.
UAT	(User Acceptance Testing) System testing done at OSFI, by the Client, where application is run through a test suite (end-to-end) to ensure that overall functionality is not broken.
SIT	(System Integration Testing) System testing done at OSFI where application is run through a test suite (end-to-end) to ensure that overall functionality is not broken.
FIT	(Functional In-board Testing) Integration testing done at OSFI where s/w is integrated into the OSFI Development environment to ensure that it is functioning as expected and that it interoperates with other tools/applications as required
Sanity	Specific testing done to ensure that major components of an application are functioning as software loads are built.
Application Program Interface (API)	A set of routines, protocols, and tools for building software applications and interacting with other applications.
Attribute	A piece of information about a Configuration Item. Examples are: name, location, version number and cost. Attributes of CIs are recorded in the Configuration Management Database (CMDB).

Term or Acronym	Definition
Contractor Facility	A Data Centre used by the Contractor or any of its subcontractors to store any of Canada's Data or otherwise deliver the ITSM Managed Service.
Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT service. Information about each CI is recorded in a configuration record within the CMDB and is maintained throughout its lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and SLAs.
Demand Management	Activities that seek to understand and influence customer demand for services and the provision of capacity to meet these demands. At a strategic level, Demand Management can involve analysis of patterns of business activity and user profiles. At a tactical level, it can involve use of differential charging to encourage customers to use IT services at less busy times.
Working Days	Refers to Federal Government working days which excludes Saturday, Sunday and the following statutory holidays: a) New Year's Day[1]; b) Good Friday and Easter Monday; c) Victoria Day; d) St-Jean Baptiste Day[1]; e) Canada Day[1]; f) 1st Monday in August; g) Labour Day; h) Thanksgiving Day; i) Remembrance Day[1]; j) Christmas Day[1]; and k) Boxing Day[2]. [1]If this holiday occurs on a Saturday or Sunday, then the following Monday will be a holiday. [2] If this holiday occurs on a Saturday, then the following Monday will be a holiday. If this holiday occurs on a Sunday or Monday, then the following Tuesday will be a holiday.
General Users	A class of Users who have general access to the ITSM Tool.
IT Infrastructure	All of the hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support IT services. The term IT Infrastructure includes all of the Information Technology but not the associated people, processes or documentation.
N	Most recent version of the software released by the software publisher
N-1	Previous version of the software released by the software publisher.

Term or Acronym	Definition
Protected Information: Protected A, Protected B and Protected C	This refers to information that the Government of Canada treats as protected and confidential, including the following information: a) 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). b) 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). c) 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).
Service Catalog	Organized and curated collection of any and all business and information technology related services that can be performed by, for, or within an enterprise.

ITIL Process Terminology	Definition
Availability Management	The ITIL Process responsible for defining, analysing, planning, measuring and improving all aspects of the availability of IT services. Availability Management is responsible for ensuring that all IT infrastructure, processes, tools, roles, etc. are appropriate for the agreed service level targets for availability.
Capacity Management	The ITIL process responsible for ensuring that the capacity of IT services and the IT Infrastructure is able to deliver agreed service level targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT service, and plans for short-term, medium-term and long-term business requirements.
Change Management	The ITIL process responsible for controlling the lifecycle of all changes. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT services.
Configuration Management Database (CMDB)	In ITIL terminology, the Configuration Management Database is a database that contains all relevant information about each Configuration Item (CI) including the CI location, status, and also its interconnectivity with other Configuration Items. The CMDB is also used to consolidate disparate data sets and be a current and accurate source of information about data within an organization's IT environment.
Continual Service improvement	A stage in the lifecycle of an IT service and the title of one of the core ITIL publications. Continual Service Improvement is responsible for

ITIL Process Terminology	Definition
	managing improvements to IT service management processes and IT services. The performance of the IT service provider is continually measured and improvements are made to processes, IT services and IT infrastructure in order to increase efficiency, effectiveness, and cost effectiveness.
Event Management	The ITIL Process responsible for managing events throughout their lifecycle. Event Management is one of the main activities of IT operations.
High Availability	In ITIL terminology, an approach or design that minimizes or hides the effects of Configuration Item failure on the Users of an IT service. High Availability solutions are designed to achieve an agreed level of Availability and make use of techniques such as fault tolerance, resilience and fast recovery to reduce the number of incidents, and the impact of incidents.
Incident Management	The ITIL process responsible for managing the lifecycle of all incidents. The primary objective of Incident Management is to return the IT service to Users with the full suite of features and functionalities as quickly as possible.
Information Security Management	The ITIL process that ensures the confidentiality, integrity and availability of an organization's assets, information, data and IT services. Information Security Management usually forms part of an organizational approach to security management that has a wider scope than the IT service provider, and includes handling of paper, building access, phone calls, etc., for the entire organization.
Information Technology (IT)	In ITIL terminology, the use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, applications and other software. The information may include business data, voice, images, video, etc. Information Technology is often used to support business processes through IT services.
IT Service Management	In ITIL terminology, the implementation and management of quality IT services that meet the needs of a business. IT Service Management is performed by IT service providers through an appropriate mix of people, processes and Information Technology.
ITIL	A set of best practice guidance for IT service management. ITIL consists of a series of publications giving guidance on the provision of quality IT services, and on the processes and facilities needed to support them.
ITIL Process	A set of coordinated activities combining and implementing resources and capabilities in order to produce an outcome and provide value to customers or stakeholders. Customized processes within an organization are considered strategic assets when they create competitive advantage and market differentiation. They may define roles, responsibilities, tools, management controls, policies, standards, guidelines, activities and work instructions if they are needed.

ITIL Process Terminology	Definition
Knowledge Management	The ITIL process responsible for gathering, analyzing, storing and sharing knowledge and information within an organization. The primary purpose of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge.
Performance Management	The ITIL process responsible for managing day-to-day performance activities. These include monitoring, threshold detection, performance analysis and tuning, and implementing changes related to performance and capacity.
Problem Management	The ITIL process responsible for managing the lifecycle of all problems. The primary objectives of Problem Management are to prevent incidents from happening, and to minimize the impact of incidents that cannot be prevented.
Release	A Release (also referred to as a “Release Package”) consists of a single Release Unit or a structured set of Release Units. A Release Unit is a set of new, changed and/or unchanged Configuration Items, which are tested and introduced into the production environment together to implement one or several approved Changes. A release can therefore include hardware and software, documentation, processes, or other components that are essential to successfully implementing an approved change to the ITSM Tool Solution.
Release and Deployment Management	The ITIL process responsible for both release management and deployment.
Request Fulfilment	The ITIL process responsible for managing the lifecycle of all service requests.
Service Capacity Management	In ITIL terminology, this is the activity responsible for understanding the capacity of IT services. The resources used by each IT service and the pattern of usage over time are collected, recorded, and analyzed for use in the capacity plan.
Service Design	A stage in the lifecycle of an IT service. Service Design includes a number of processes and functions and is the title of one of the Core ITIL publications.
Service Level Management (SLM)	The ITIL Process responsible for negotiating service level commitments, and ensuring that these are met. SLM is responsible for ensuring that all IT service management processes, operational level agreements, and underpinning contracts, are appropriate for the agreed service level targets. SLM monitors and reports on service levels, and holds regular customer reviews.
Service Management	In ITIL terminology, Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services.
Service Management Lifecycle	In ITIL terminology, an approach to IT service management that emphasizes the importance of coordination and control across the various functions, processes, and systems necessary to manage the full lifecycle of IT services. The Service Management lifecycle

ITIL Process Terminology	Definition
	approach considers the strategy, design, transition, operation and continual improvement of IT services.
Service Operation	In ITIL terminology, a stage in the lifecycle of an IT service operation. Day-to-day management of an IT service, system, or other configuration item. Operation is also used to mean any predefined activity or transaction.
Service Portfolio Management	The ITIL process responsible for managing the service portfolio. Service Portfolio Management considers services in terms of the business value that they provide.
Service Strategy	The title of one of the core ITIL publications. Service Strategy establishes an overall strategy for IT services and for IT Service Management.
Service Transition	A stage in the lifecycle of an IT service. Service Transition includes a number of processes and functions and is the title of one of the Core ITIL publications.
Supplier Management	The ITIL process responsible for ensuring that all contracts with suppliers support the needs of the business, and that all suppliers meet their contractual commitments.

APPENDIX 4 – SECURITY CONTROLS

Legend	
Security Control ID	Cross-reference to the applicable Security Control. For a detailed description of Security Control, please refer to • Annex 3A - Security Control Catalogue and • Annex 4A - Profile 1 - (PROTECTED B / Medium Integrity / Medium Availability) These documents are available at the CSE web site: https://www.cse-cst.gc.ca/en/publication/itsg-33 https://www.cse-cst.gc.ca/fr/publication/itsg-33
SSC responsible to address for the Infrastructure level	A marking in this column means that SSC is responsible to address this security element when providing a base platform (OS and other elements) in SSC Data Centre(s)
Vendor Responsible to Address for the Application Layer	A marking in this column means the vendor is responsible to address this security element with SSC providing a base platform (OS and other elements) in SSC Data Centre(s)
AICPA SSAE 16 SOC2	A marking in this column means this security element forms part of this industry standard
ISO / IEC 27001	A marking in this column means this security element forms part of this industry standard

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
AC-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.9.1.1 A.12.1.1 A.18.1.1 A.18.2.2
AC-2	X	X	CC5.2 CC6.1	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.5 A.9.2.6
AC-2 (1)	X	X	CC5.2	
AC-2 (2)	X	X	CC5.2	

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
AC-2 (3)	X	X	CC5.2	
AC-2 (4)	X	X	CC5.2	
AC-2 (5)	X	X	CC5.3	
AC-2 (7)	X	X	CC5.4	
AC-2 (12)	X		CC6.1	
AC-3	X	X	CC5.1	A.6.2.2 A.9.1.2 A.9.4.1 A.9.4.4 A.9.4.5 A.13.1.1 A.14.1.2 A.14.1.3 A.18.1.3
AC-3 (9)	X	X		
AC-4	X	X	CC5.1	A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3
AC-5	X	X	CC5.1	A.6.1.2
AC-6	X	X	CC5.4	A.6.1.2
AC-6 (1)	X	X	CC5.4	
AC-6 (2)	X	X	CC5.1	
AC-6 (5)	X	X	CC5.4	
AC-6 (7)	X	X		
AC-6 (9)	X	X	CC6.1	
AC-6 (10)	X	X	CC5.1	
AC-7	X	X	CC5.3	A.6.1.2
AC-8	X	X	CC2.3	A.6.1.2
AC-10	X	X	CC5.3	
AC-11	X	X	CC5.3	A.11.2.8 A.11.2.9
AC-11 (1)	X	X	CC5.3	
AC-12	X	X	CC5.3	
AC-14	X	X	CC5.1	

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
AC-20	X	X	CC2.3	A.11.2.6 A.13.1.1 A.13.2.1
AC-20 (1)	X	X	CC5.6	
AC-20 (3)	X	X		
AC-21	X	Information sharing by Vendor is Prohibited	CC5.4	
AC-22	X	X	CC5.4	
AT-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
AT-2	X	X	CC2.3	A.7.2.2.2 A.12.2.1
AT-2 (2)	X	X	CC1.3 CC2.5	
AT-3	X	X	CC2.3	A.7.2.2*
AT-4	X	X	CC2.3	
AU-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
AU-2	X	X	CC6.1	
AU-2 (3)	X	X	CC6.1	
AU-3	X	X	CC6.1	A.12.4.1*
AU-3 (1)	X	X	CC6.1	
AU-4	X	X	CC6.1	A.12.1.3
AU-4 (1)	X	X	CC6.1	
AU-5	X	X	CC6.1	
AU-6	X	X	CC6.1	A.12.4.1 A.16.1.2 A.16.1.4
AU-6 (1)	X	X	CC6.1	

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
AU-6 (3)	X	X	CC6.1	
AU-6 (4)	X	X	CC6.1	
AU-7	X	X	CC6.1	
AU-7 (1)	X	X	CC6.1	
AU-8	X	X	CC6.1	A.12.4.4
AU-8 (1)	X	X	CC6.1	
AU-9	X	X	CC6.1	A.12.4.2 A.12.4.3 A.18.1.3
AU-9 (2)	X	X	CC6.1	
AU-9 (4)	X	X		
AU-9 (6)	X	X		
AU-11	X	X	CC6.1	A.12.4.1 A.16.1.7
AU-12	X	X	CC6.1	A.12.4.1 A.12.4.3
AU-12 (1)	X	X	CC6.1	
CA-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
CA-2	X	X	CC4.1	A.14.2.8 A.18.2.2 A.18.2.3
CA-2 (1)	X	X	CC4.1	A.18.2.1 E
CA-2 (2)	X		CC4.1	
CA-2 (3)	X	X	CC4.1	
CA-3	X	X	CC7.1	A.13.1.2 A.13.2.1 A.13.2.2
CA-3 (3)	X	X	CC7.1	
CA-3 (5)	X	X	CC5.6	
CA-5	X	X	CC4.1	

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
CA-6	X	X	CC7.4	
CA-7	X	X	CC4.1	
CA-7 (1)	X	X	CC4.1	
CA-8	X		CC4.1	
CA-8 (1)	X		CC4.1	
CA-9	X	X	CC7.1	
CM-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
CM-2	X	X	CC7.4	
CM-2 (1)	X	X	CC7.2 CC7.3 CC7.4	
CM-2 (2)	X	X	CC7.4	
CM-3	X	X	CC7.4	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4
CM-3 (2)	X	X		
CM-3 (4)	X	X	CC7.1	
CM-3 (6)	X	X	CC7.4	
CM-4	X	X	CC7.1	A.14.2.3
CM-4 (2)	X	X		
CM-5	X		CC7.4	A.9.2.3 A.9.4.5 A.12.1.2 A.12.1.4 A.12.5.1
CM-5 (1)	X		CC7.4	
CM-5 (2)	X	X		
CM-5 (5)	X		CC7.4	
CM-6	X	X	CC5.1 CC7.4	

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
CM-6 (1)	X	X	CC7.4	
CM-7	X	X	CC5.1 CC7.1	A.12.5.1*
CM-7 (1)	X	X	CC7.3	
CM-7 (2)	X	X	CC5.1	
CM-7 (5)	X		CC5.1	A.12.5.1 E
CM-8	X	X	CC5.1	A.8.1.1 A.8.1.2
CM-8 (1)	X	X	CC7.4	
CM-8 (3)	X	X	CC6.1 CC6.2	
CM-8 (5)	X	X	CC7.4	
CM-8 (6)	X	X		
CM-9	X	X	CC7.4	A.6.1.1*
CM-10	X	X	CC3.1	A.18.1.2
CM-10 (1)	X	X	CC3.1	
CM-11	X	X	CC5.8	A.12.5.1 A.12.6.2
CM-11 (1)	X	X		
CM-11 (2)	X	X		
CP-1	X	X	CC3.1 CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
CP-2	X	X	CC3.1 CC3.3	A.6.1.1 A.17.1.1 A.17.2.1
CP-2 (1)	X	X	CC3.1	
CP-2 (2)	X	X	A1.1	A.12.1.3 E
CP-2 (3)	X	X	CC3.1	
CP-2 (4)	X	X		
CP-2 (5)	X	X		

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
CP-2 (6)	X	X		
CP-2 (8)	X	X	CC3.1	
CP-3	X	X	CC1.3	A.7.2.2*
CP-4	X	X	A1.3	A.17.1.3
CP-4 (1)	X	X	A1.3	
CP-10	X	X	CC3.1	A.17.1.2
IA-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
IA-2	X	X	CC5.3	A.9.2.1
IA-2 (1)	X	X	CC5.3	
IA-2 (2)	X	X	CC5.3	
IA-2 (3)	X	X	CC5.3	
IA-2 (8)	X	X	CC5.3	
IA-2 (9)	X	X	CC5.3	
IA-2 (11)	X	X	CC5.3	
IA-3	X	X	CC5.1	
IA-4	X	X	CC5.1 CC5.2	A.9.2.1
IA-4 (4)	X	X	CC5.2	
IA-5	X	X	CC5.1 CC5.2 CC5.3	A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.3
IA-5 (1)	X	X	CC5.1 CC5.3	
IA-5 (2)	X	X	CC5.1 CC5.3	
IA-5 (3)	X	X	CC5.2	
IA-5 (6)	X	X	CC5.1	
IA-5 (7)	X	X	CC5.1 CC7.1	

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
IA-5 (9)	X	X		
IA-6	X	X	CC5.3	A.9.4.2
IA-7	X	X	CC5.1	A.18.1.5
IA-8	X	X	CC5.3	A.9.2.1
IA-8 (100)	X	X		
IR-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
IR-2	X	X	CC1.3	A.7.2.2*
IR-3	X	X	CC6.2	
IR-3 (2)	X	X	CC6.2	
IR-4	X	X	CC6.2	A.16.1.4 A.16.1.5 A.16.1.6
IR-4 (4)	X	X	CC6.2	
IR-4 (8)	X	X	CC6.2	
IR-3 (2)	X	X	CC6.2	
IR-5	X	X	CC6.2	
IR-6	X	X	CC6.1	A.6.1.3 A.16.1.2
IR-6 (2)	X	X	CC6.2	
IR-7	X	X	CC6.1	
IR-8	X	X	CC6.2	A.16.1.1
IR-9	X	X	CC6.2	
IR-9 (1)	X	X	CC6.2	
IR-9 (2)	X	X	CC1.3	
IR-9 (3)	X	X	A1.2	
IR-9 (4)	X	X	CC2.3	
IR-10	X	X		
MA-1	X	X	CC3.2	A.5.1.1 A.5.1.2

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
				A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
MA-2	X	X	CC5.6 CC7.1	A.11.2.4* A.11.2.5*
MA-3	X	X	CC7.1	
MA-3 (1)	X	X	CC5.6	
MA-3 (2)	X	X	CC5.8	
MA-3 (3)	X	X	CC5.6	
MA-4	X	X	CC5.1 CC5.3 CC6.1	
MA-4 (2)	X	X	CC7.4	
MA-4 (4)	X	X		
MA-4 (6)	X	X	CC7.4	
MA-5	X	X	CC1.4 CC5.6	
MA-5 (1)	X	X	CC7.4	
MA-5 (5)	X	X		
MA-6	X	X	A1.2	A.11.2.4
PL-1	X	X	CC3.1 CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
PL-2	X	X	CC3.1 CC3.3	A.14.1.1
PL-2 (3)	X	X	CC3.1	
PL-4	X		CC2.3	A.7.1.2 A.7.2.1 A.8.1.3
PL-4 (1)	X	X	CC2.3	
PL-7	X	X		A.14.1.1*
PL-8	X	X	CC3.2	A.14.1.1*

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
PL-8 (1)	X	X	CC5.1	
PS-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
PS-2	X	X	CC1.4	
PS-3	X	X	CC1.4	A.7.1.1
PS-4	X	X	A1.2 CC5.2 CC5.4 CC5.6	A.7.3.1 A.8.1.4
PS-5	X	X	CC5.4 CC5.5	A.7.3.1 A.8.1.4
PS-6	X	X	CC1.4	A.7.1.2 A.7.2.1 A.13.2.4
PS-7	X	X	CC1.2 CC1.4 CC4.1 CC5.5	A.6.1.1* A.7.2.1*
PS-8	X	X	CC1.1	A.7.2.3
RA-1	X	X	CC3.1	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
RA-2	X		CC3.1	A.8.2.1
RA-3	X		CC3.1	A.12.6.1*
RA-5	X		CC4.1	A.12.6.1*
RA-5 (1)	X		CC4.1	
RA-5 (2)	X		CC4.1	
RA-5 (3)	X	X	CC4.1	
RA-5 (5)	X		CC4.1	
RA-5 (6)	X		CC4.1	

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
RA-5 (8)	X		CC4.1	
SA-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
SA-2	X	X	CC1.3 CC3.3	
SA-3	X	X	CC7.1 CC7.4	A.6.1.1 A.6.1.5 A.14.1.1 A.14.2.1 A.14.2.6
SA-4	X	X	CC7.1	A.14.1.1 A.14.2.7 A.14.2.9 A.15.1.2
SA-4 (1)	X	X	CC7.1	
SA-4 (2)	X	X	CC7.1	
SA-5	X	X	CC1.3 CC5.1 CC7.1	A.12.1.1*
SA-8	X	X	CC7.1	A.14.2.5
SA-9	X	X	CC4.1	A.6.1.1 A.6.1.5 A.7.2.1 A.13.1.2 A.13.2.2 A.15.2.1 A.15.2.2
SA-9 (1)	X	X	CC7.1	
SA-9 (2)	X	X	CC7.1	
SA-9 (3)	X	X		
SA-9 (4)	X	X	CC3.1	
SA-9 (5)	X	X	CC5.5	
SA-10	X	X	CC7.1 CC7.4	A.12.1.2 A.14.2.2

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
				A.14.2.4 A.14.2.7
SA-10 (1)	X	X	CC7.1	
SA-11	X	X	CC7.1	A.14.2.7 A.14.2.8
SA-11 (1)	X	X	CC7.1	
SA-11 (2)	X	X	CC7.1	
SA-11 (5)	X	X		
SA-11 (7)	X	X		
SA-11 (8)	X	X	CC7.1	
SA-12	X			A.14.2.7 A.15.1.1 A.15.1.2 A.15.1.3
SA-15	X			A.6.1.5 A.14.2.1
SA-16	X	X		
SA-17	X	X		A.14.2.1 A.14.2.5
SA-17 (2)	X	X		
SA-17 (7)	X	X		
SA-18	X	X		
SA-18 (1)	X	X		
SA-22	X			
SA-22 (1)	X	X		
SC-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
SC-2	X	X	CC5.1	
SC-5	X		CC5.1	
SC-6	X	X		

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
SC-7	X		CC5.1 CC5.6	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.3
SC-7 (3)	X		CC5.6	
SC-7 (4)	X		CC5.6	
SC-7 (5)	X		CC5.6	
SC-7 (7)	X		CC5.6	
SC-7 (8)	X		CC5.6	
SC-7 (9)	X			
SC-7 (11)	X		CC5.6	
SC-7 (12)	X		CC5.6	
SC-7 (13)	X		CC5.6	
SC-7 (18)	X		CC5.6	
SC-8	X	X	CC5.7	A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3
SC-8 (1)	X	X	CC5.7	A.18.1.3
SC-8 (2)	X	X		
SC-10	X	X	CC5.1 CC5.6	A.13.1.1
SC-12	X	X	CC5.1	A.10.1.2
SC-12 (1)	X	X		
SC-12 (2)	X	X	CC5.1	
SC-12 (3)	X	X	CC5.1	
SC-13	X	X	CC5.1	A.10.1.1 A.14.1.2 A.14.1.3 A.18.1.5
SC-17	X	X	CC5.1	A.10.1.2
SC-18	X	X	CC5.8	
SC-19	X	X	CC5.1	

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
SC-20	X	X	CC5.1 CC5.6	
SC-21	X	X	CC5.1	
SC-22	X	X	A1.1	
SC-23	X	X	CC5.1 CC5.3	
SC-23 (1)	X	X	CC5.3	
SC-23 (3)	X	X	CC5.3	
SC-23 (5)	X	X		
SC-28	X	X	CC5.1	A.8.2.3*
SC-28 (1)	X	X		
SC-39	X	X	CC5.1	
SI-1	X	X	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
SI-2	X	X	CC6.1 CC6.2 CC7.3	A.12.6.1 A.14.2.2 A.14.2.3 A.16.1.3
SI-3	X		CC5.8	A.12.2.1
SI-3 (1)	X		CC5.8	
SI-3 (2)	X		CC5.8	
SI-3 (4)	X			
SI-3 (7)	X		CC5.8	
SI-4	X		CC3.2 CC6.1	
SI-4 (1)	X		CC6.1	
SI-4 (2)	X		CC6.1	
SI-4 (4)	X		CC6.1	
SI-4 (5)	X		CC6.1	
SI-4 (7)	X			

Security Control ID	SSC responsible to address for the Infrastructure Level	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001
SI-4 (9)	X			
SI-4 (11)	X			
SI-4 (12)	X		CC6.1	
SI-4 (13)	X			
SI-4 (16)	X		CC6.1	
SI-5	X	X	CC6.1 CC7.3	A.6.1.4*
SI-6	X		CC6.1 CC6.2	
SI-7	X	X	CC6.1	
SI-7 (1)	X	X	CC6.1	
SI-7 (2)	X	X		
SI-7 (7)	X	X	CC6.1	
SI-7 (14)	X	X		
SI-8	X		CC5.8	
SI-8 (1)	X		CC5.8	
SI-8 (2)	X	X	CC5.8	
SI-10	X	X	PI1.2	
SI-11	X	X	PI1.1	
SI-12	X	X	PI1.4	
SI-16	X	X	CC5.1	