Service | Innovation | Value

INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM) TOOL IMPLEMENTATION SERVICES

ANNEX A

STATEMENT OF WORK (SOW)

Draft v7

February 26, 2018

Contents

1 INTRODUCTION

Shared Services Canada (SSC) has established the SSC Service Management Transformation Program that is aimed at fundamentally transforming SSCs Information Technology Service Management (ITSM) capabilities. SSC requires the services of a Contractor to supply, implement and support a complete Enterprise ITSM Tool solution comprised of:

- Enterprise ITSM Tool COTS software;
- System Integration professional services required to implement the new ITSM Tool solution;
- Transition-out Services; and
- Application Management Services.

The solution will be implemented on premise, on SSC provided infrastructure, at GC Enterprise Data Centre Services locations. The Contractor's Work requirements are described in sections 4 – 16 of this SOW.

2 BACKGROUND

2.1 Shared Services Canada (SSC)

SSC is mandated to simultaneously operate and transform the Government of Canada's Information Technology (IT) infrastructure including email, data center and network services. SSC is responsible for the IT infrastructure for 43 departments and agencies and currently delivers services to over 300,000 users across the GC. Although SSC's first obligation is to ensure the sustainability of this infrastructure, it is also responsible to transform the existing environment into a consolidated enterprise model for the whole of Government.

2.2 Service Management Transformation

2.2.1 Service Management Transformation Program Overview

SSC has embarked on a multi-year journey to fundamentally transform its capabilities, with Service Management being core components of the transformation. To ensure its services meet the requirements of customers, SSC is implementing a comprehensive service strategy that sets out how it will deliver enterprise IT infrastructure services, including roles and responsibilities and service targets. Central to this work is the launch of the SSC Service Management Transformation Program that is aimed at fundamentally transforming SSC ITSM capabilities. The Program is focused on:

- Delivering an enterprise ITSM technology solution
- Accelerating the evolution of existing and development of new ITIL-based processes
- Driving enterprise adoption of new tools and processes through a comprehensive organizational change management program.

An end-to-end Information Technology Service Management (ITSM) Process Evolution assessment completed in 2015 formed the basis of the business case for the establishment of the Service Management Transformation Program and related funding.

- **Legacy Migration Project** – is advancing the consolidation of SSC support resources to one legacy ITSM ticketing tool, Enterprise Control Desk (ECD). This project is enabling SSC to better manage IT infrastructure by driving adoption of standardized service management processes. The consolidation to the existing tool will help ready SSC for the implementation of and migration to a new Service Management Tool. To date, 28 departments representing 25-30% of SSC tickets are leveraging the ECD tool.
- **Configuration Management Database Enhancement** – is an initiative to advance the maturity of this crucial database, and enhance the configuration information available to support Incident and Change Management. This work will also help ready SSC for the implementation of the new Service Management Tool.
- **ITSM Process Evolution** – is the multi-year initiative to establish enterprise-wide ITSM processes. This initiative is the core of the Service Management Transformation Program and will address the key challenges faced by SSC with regards to its fragmented operating environment, challenges in implementing enterprise processes, and inefficiency in generating effective performance reports.

  Note: A contract was awarded in October 2017 for ITSM Process Maturity Solution services required to collaborate, plan, manage and deliver a fully integrated set of ten ITSM processes, backed by an organizational structure to support these processes, within SSC. There is a significant Organizational Change Management (OCM) component to the work to be delivered by the ITSM Process Maturity Solution contractor.

  The ITSM Process Maturity Solution contractor is responsible for developing and documenting the detailed Functional Requirements for each ITSM process, from which the Contractor (described herein) will develop the Design Specifications and configure each ITSM process in the Tool.
- **Enterprise ITSM Tool Project** – is a multi-year project to establish an enterprise-wide ITSM solution. This project will directly support the other program initiatives by providing an Enterprise ITSM solution to be configured and deployed to production by a vendor in order to support SSC service management activities.

  Note: The evolution of SSC's ITSM Process and implementation of the new Enterprise ITSM Tool, will be accomplished collaboratively between SSC, the ITSM Process Maturity Solution contractor, and the Contractor (described herein). The envisioned collaborative process, including roles and responsibilities of each contributor, are more fully described in section 3.4 below.
- **Expansion of Capacity** - is also being enhanced in key areas to address resourcing issues and gaps in operational areas and to enable improved service delivery and customer satisfaction.

The Service Management Transformation Program also features a number of future year initiatives that would help advance the service management transformation agenda. Their implementation and funding are only forecasted in future years.

Through a phased approach, the goal is to stand up an effective service management function and implement mature ITSM processes to maximize efficiencies, simplify workflows, and enhance the quality of services SSC delivers to its customer organizations.

2.2.2 ITSM Process Design Priorities

SSC's Service Management Transformation Program will include the design and implementation of ten ITSM processes, listed below, as prioritized by SSC. The ITIL best practice framework for IT Service Management will be used to define and provide guidance for the ITSM processes to be transformed under the Service Management Transformation Program.

ITSM Process Grouping	
Release Package A (Core Processes)	Service Asset Configuration Management including CMDB design
	Incident Management
	Request Fulfillment
	Change Management
Release Package B	Service Catalogue Management including Service Catalogue design
	Service Level Management
	Event Management
Release Package C	Knowledge Management
	Problem Management
	Release and Deployment Management
Optional Processes	Demand Management
	Capacity Management
	IT Financial Management
	Availability Management

The new redesigned ITSM Processes (as delivered by the ITSM Process Maturity Solution contractor) will be configured in the enabling Enterprise ITSM Tool, by the Contractor. Refer to section 3.4 for further details of the collaborative process.

SSC currently anticipates the delivery of 10 configuration-ready processes, to at minimum Lean[1] level, as follows:

- Release Package A: Fall 2018 (Q3)
- Release Package B: Winter 2019 (Q4)
- Release Package C: Spring 2019 (Q1)

For each process, within the three release packages, the goal is to get them to a Mature[2] state within 30 months.

Notes: 1. Lean meaning that the highest value items identified through a SSC business and operational needs assessment of the in scope processes have been addressed to deliver basic functionality for the process that does not already exist or is limited. 2. 'Mature' meaning that the overall objectives for process improvement have been met.

3 ENTERPRISE ITSM TOOL PROJECT

3.1 Current State

3.1.1 SSC

At inception in 2011, SSC inherited disparate systems and processes, which resulted in a highly reactive operating environment with no consistency in response, service restoration and request fulfillment. Incomplete visibility to workload, productivity and performance persists, impacting performance measurement and reporting.

In order for the SSC Service Delivery and Management Branch program to achieve its business outcomes, a requirement has been identified to replace SSC's current ITSM Toolset [including, but not limited to IBM's Enterprise Control Desk (ECD)] with a modern, scalable, ITSM solution.

In addition to the ITSM Toolset in use at SSC, there are a variety of ITSM tools in use at SSC's customer departments. Currently, end-users log IT problems and requests via their established departmental support structure (e.g. Departmental Help Desk) and a ticket is created in the departmental tracking system. Using a desk-to-desk model, applicable IT issues are escalated to SSC via a telephone call from the customer department to SSC's Enterprise Service Desk where a ticket is logged in SSC's ECD system. Currently, there is no mechanism to effectively track IT issues end-to-end from the originating customer department through to resolution at SSC.

The current Enterprise Control Desk (ECD) system has a number of integrations with different systems and applications across SSC and some Customers as described in more detail below.

Refer to the SSC Infrastructure Services Overview, provided as Appendix 9, for further details.

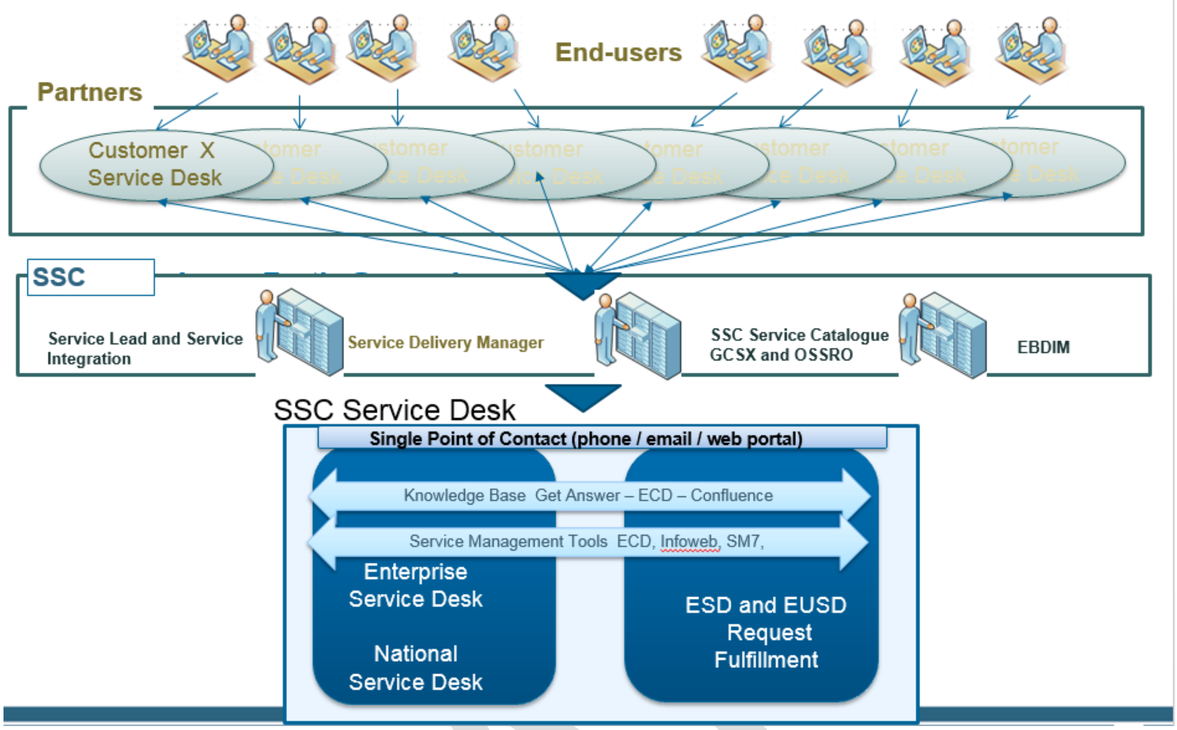
3.1.2 Customer Departments/Agencies

Using the current ITSM Toolset, the SSC Enterprise Service Desk (ESD) provides support for SSC infrastructure services and some legacy client desktop services for multiple GC customer department/agencies (43), including SSC itself. The ESD acts as the entry point into SSC for service requests and incidents to either fulfill, resolve or coordinate the resolution with SSC service lines and vendors. As part of SSC's desk-to-desk model, GC end-users are required to initiate contact with their departmental Service Desk who, using a variety of ITSM tools, create a ticket in their system. Customer departments are responsible for managing application-related incidents and service requests. If the department Service Desk determines that the incident or service request is related to an SSC service, the Service Desk will escalate the ticket to the SSC ESD often via a telephone call or entry of the ticket information in the SSC ECD system (e.g. swivel chair). Currently, there is no mechanism to effectively track incidents and service requests end-to-end from the originating customer through to SSC resolution.

The ECD system has a number of integrations with different systems and application across SSC and some customers as described in more detail in Section 11. Refer to Appendix 7 for a list of the ITSM Tools currently in use at SSC and customer departments.

Further to this, there are approximately 850 SSC staff still embedded in their originating customer department/agency, who utilize customer ITSM processes and tools to delivery SSC services.

For select SSC services, GC customers/users submit service requests for processing directly via a portal (e.g. ECD, Serving Government website).


End-users
Partners
Customer X Service Desk
SSC
Service Lead and Service Integration
Service Delivery Manager
SSC Service Catalogue GCSX and OSSRO
EBDIM
SSC Service Desk
Single Point of Contact (phone / email / web portal)
Knowledge Base Get Answer – ECD – Confluence
Service Management Tools ECD, Infoweb, SM7,
Enterprise Service Desk
National Service Desk
ESD and EUSD Request Fulfillment

In the short to mid-term SSC will retain the desk-to-desk model with plans to increase opportunity for GC customer/users to initiate tickets directly to SSC through a self-service portal. At the same time, SSC will continue to integrate SSC and customer ITSM processes and establish a bi-directional interface with customer ITSM tools.

3.2 Target Solution

3.2.1 Long-term Vision

The ITSM Tool selected and implemented as part of the ITSM Tool Solution will provide a foundation for establishing GC-wide standards, processes and tools. This foundation will provide the opportunity for the GC to establish a single GC IT support model; where by GC end-users contact a central point (e.g.1-800-GCIT, GC self-service portal) and their request is routed to the appropriate department, group, etc.

Ideally, all customers will ultimately fully transition to the new ITSM solution to both manage both their own application-related tickets as well as refer tickets to SSC.

3.2.2 Target Operating Model

The high-level requirements and objectives for the new ITSM Solution are summarized as follows:

Requirement	Description
GC Enterprise ITSM Solution	Standardized enterprise IT Service Management (ITSM) processes supported by an industry leading ITSM tool that can be leveraged by SSC customers with support for multi-tenancy and multi instance as well as standard APIs with other ITSM tools. Solution scope must support all active SSC Catalogue services.
ITSM Process Modules	ITSM tool includes process modules that support each of the in-scope Process Maturity Solution contract processes and has the capability to enable and support other ITSM processes such as Service Authorization and Service Portfolio Management and associated performance reporting.
GC Requirements	Adheres to GC requirements including official languages, Web Content Accessibility Guidelines (WCAG), privacy and security for Protected B Medium integrity and Medium availability (PBMM) obligations and standards.
Self Service Portal	User-centric self-service portal that allows end-users to submit incidents and service requests, view status, receive broadcast notifications/communications and search FAQ information/knowledge base.
Role-based Access and Functionality	ITSM Solution permits the separation of users based on role and access to certain functionality based on role (e.g. access and permissions).
Visibility of Shared Information	ITSM Solution provides SSC and customer real time visibility of shared ticket and CI information to understand departmental-wide impacts/dependencies of outages and planned change activity.
Business Analytics	Ability to easily construct queries and reports from any combination of database fields and tables, report on discrete key performance indicators (KPIs), correlate KPIs from multiple processes into a consolidated view and analyze trends over time.
Protection of Upgrade Path	Flexibility to configure process workflows within the tool to meet SSC and customer business needs while ensuring the upgrade path is always maintained
Auto-Discovery Capability	ITSM solution provides a centralized module for identifying and reconciling CMDB CI data from different data sources. It must support multiple data sources such as Discovery, import sets, and manual entries that are used to create and update CI records.
Multi-channel / Multiplatform Capability	Multi-channel, multiplatform capability (e.g. chat, cross platform access: mobile, tablet, PC).

Requirement	Description
Email interface	Email interface to create and update tickets and approve requests
Interface Mechanisms	Ability of ITSM tool to interface through industry standard mechanisms (SOAP/Web Services, REST API, etc.) with known SSC/Customer toolsets (e.g. SCOM, CA Spectrum, Sigma, etc.) and other ITSM toolsets.
Application Availability	Minimum 99.5% availability 24/7 x 365
ITSM Solution Support	ITSM Solution support must be available to SSC 24 hours/day, 365 days/year in both official languages.

Under the multi-year Enterprise ITSM Tool Project, the Contractor will provide and support an ITSM Tool solution (including COTS Enterprise ITSM Tool software and IM/IT services as set out herein), to be implemented on premise, on SSC provided infrastructure, at GC Enterprise Data Centre Services locations. The ITSM Tool Solution will be implemented to support SSC's service management requirements, including bi-directional interfaces with legacy ITSM tools in use at customer organizations and the conversion and migration of SSC's legacy data to the new Tool.

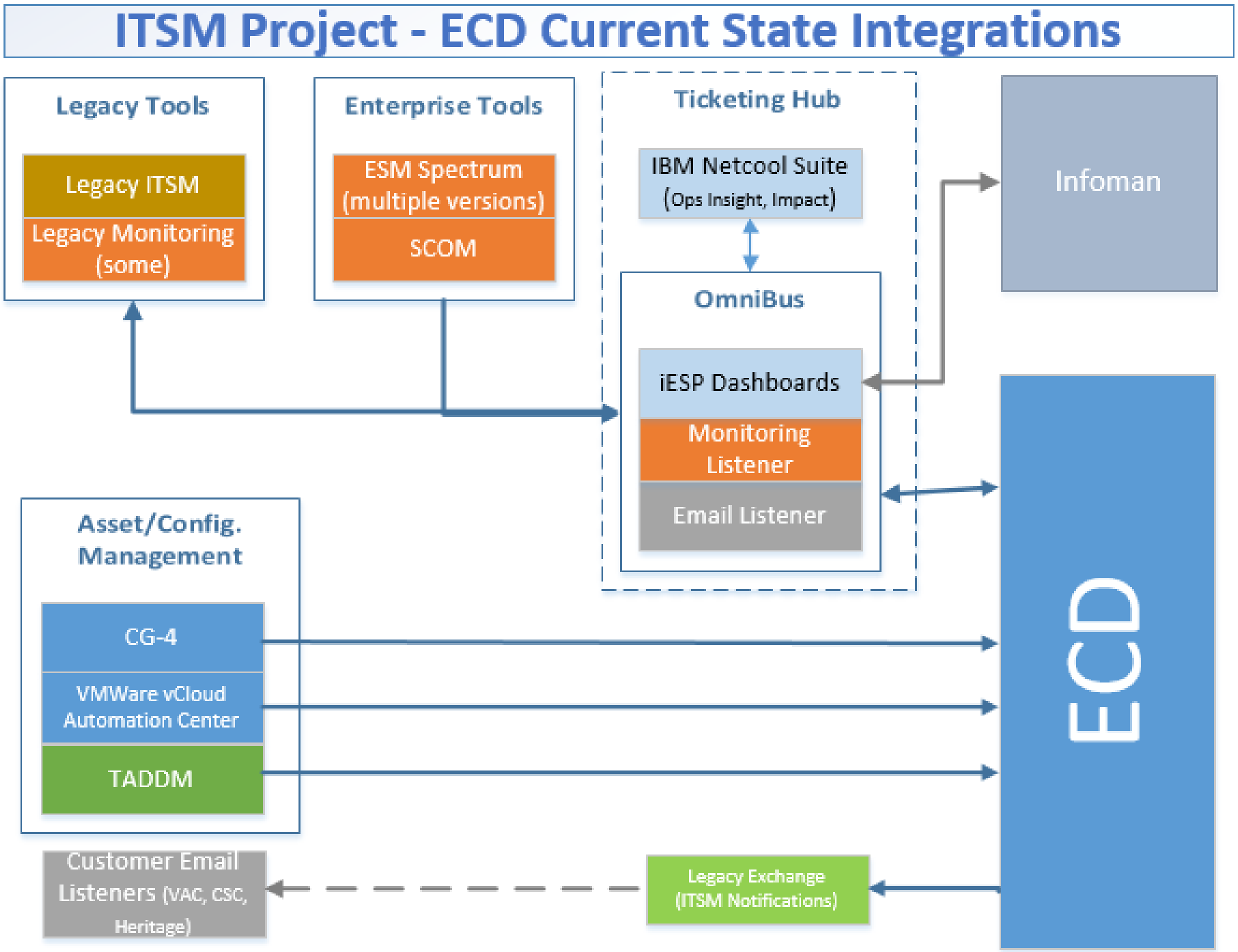
SSC customers and their users will primarily interact with SSC for service management requirements. However, the ITSM Tool Solution must include self-service features and functionalities available to General Users for the purpose of, for example, reporting incidents, submitting service requests, and performing other general User functions as depicted in the Conceptual Architecture below.

Although the ITSM Tool Solution will be implemented, initially, to support SSC's service management requirements, the Solution must be capable of supporting multi-tenant instances as it is anticipated that the Solution may be expanded to SSC customer organizations to support their own departmental ITSM requirements.

3.2.3 Integration Requirements

SSC's current Enterprise Control Desk (ECD) system has a number of integrations with different systems and applications across SSC and some Customers as depicted in the following graphic and described more detail below.

Diagram 1 – Current State


ITSM Project - ECD Current State Integrations
Legacy Tools
Legacy ITSM
Legacy Monitoring (some)
Enterprise Tools
ESM Spectrum (multiple versions)
SCOM
Ticketing Hub
IBM Netcool Suite (Ops Insight, Impact)
OmniBus
iESP Dashboards
Monitoring Listener
Email Listener
Infoman
ECD
Asset/Config. Management
CG-4
VMWare vCloud Automation Center
TADDM
Customer Email Listeners (VAC, CSC, Heritage)
Legacy Exchange (ITSM Notifications)

SSC anticipates that the functionality of the new Enterprise ITSM Tool will replace some of the current integration requirements. Further, due to the evolving business environment at SSC, some of the existing integration requirements may be implemented differently in the new Enterprise ITSM Tool to leverage the Tool's features and capabilities (i.e. Legacy Email Exchange vs Your-Email-Service). In addition, some of the integrations in the current state are workarounds for functionality not present in the ECD system that will be replaced or added through fulfilling stated requirements for the new ITSM Solution (e.g. Procurement and Asset Tracking System (PATS) integration).

The existing ECD integration landscape and the anticipated integration requirements under the new Enterprise ITSM Tool Solution are further detailed in the table below. The Contractor will complete the analysis of the systems listed below and propose the way forward.

Table 1 – Integration Summary

Current Integrated System / Application	Existing Integration (as-is)	Integration Required (future state)
Tivoli OmniBus - IESP Dashboards	Yes	No
Tivoli OmniBus - Email Listener Probes	Yes - indirect via OmniBus	No
Tivoli OmniBus - ESM Spectrum	Yes - indirect via OmniBus	Yes – between ESM Spectrum and new tool (bypass OmniBus)
Tivoli OmniBus – SCOM	Yes - indirect via OmniBus	Yes - between SCOM and new tool (bypass Omnibus)
Microsoft Exchange (Legacy Email Exchange)	Yes	No – replaced by bidirectional ticket interface in new tool
Customer Email Listeners	Yes	No – replaced by bidirectional ticket interface in new tool
CG-4 Barcode Scanning Solution	Yes	Yes
VCAC VMWare vCloud Automation Centre	Yes	TBD
Tivoli Application Dependency Discovery Manager	Yes	TBD
Procurement and Asset Tracking System (PATS)	Yes	TBD – acts as go-between for P2P and Sigma, may be best to integrate directly
P2P	Yes – indirect via PATS	TBD
SIGMA	Yes – indirect via PATS	TBD
ITOP (CMDB Staging Server):	No – planned in near future	Yes

Note: Refer to section 11 for additional details.

3.2.4 Rollout Strategy

3.2.4.1 SSC and Pilot Department

Initially, the ITSM Tool Solution will be implemented to support SSC as well as a designated customer department/agency (Pilot customer – TBA) as a tenant on the SSC instance.

3.2.4.2 Onboarding of Additional Departments

The expansion of the ITSM Tool Solution to individual customer organizations, is depicted in the graphic below, and could include:

a) Scaling of the ITSM Tool Solution (including additional Software licences and SSC provided hardware capacity) as required to support onboarding of the customer **as a tenant on SSC's multi-tenant**

instance. (**Note:** SSC will leverage its re-designed processes and configured Tool to support on-boarding of the customer department/agency); and/or

b) Scaling of the ITSM Tool Solution (including additional Software licences and SSC provided hardware capacity) as required to support onboarding of the customer to a **separate instance** of the solution and configuration of the ITSM tool as required. (**Note:** The customer department/agency must adhere to process integration standards and is responsible for their own organization's ITSM process design/maturity).

3.2.5 Establishment of Standards

The Enterprise ITSM Tool selected and implemented as part of the ITSM Tool Solution will establish the Departmental ITSM software standard for SSC.

In addition, the ITSM Tool Project will also provide a foundation for establishing GC-wide ITSM standards, processes, and tools:

- Repository of standard SSC ITSM processes, including interfaces to customer ITSM processes.
- ITSM process information exchange standards being defined by the GC ITSM Working Group (CIO/GC-EARB update planned for early 2018) to support an SSC-level standard.
- The Enterprise ITSM Tool selected and implemented under this Contract may, in the future, establish the common software standard for the Government of Canada.

3.2.6 Migration to Cloud

In the longer-term, SSC may, at its option, elect to migrate the ITSM Tool Solution to an on premise cloud environment.

3.3 Volumetric Data

3.3.1 ITSM Record Volumes

3.3.1.1 SSC

The estimated number of ITSM records representing SSC's ITSM workload is summarized in the table that follows:

Record Type	Quantity (per year)	Description
Service Requests	*TBD*	Estimated number of service requests received by SSC across Government.
Incidents	*TBD*	Estimated number of incidents reported to and/or managed by SSC across Government.
Change Requests	*TBD*	Estimated number of change requests reported to and/or managed by SSC across Government.
Configuration Items (CMDB records)	82,000	Refers to the number of CIs specifically. This doesn't take into account potential records representing relationships between CIs.

3.3.1.2 Pilot Department

The estimated number of ITSM records representing the Pilot Department's ITSM workload is summarized in the table that follows:

Record Type	Quantity (per year)	Description
Service Requests	*TBD*	Estimated number of service requests received.
Incidents	*TBD*	Estimated number of incidents reported.
Configuration Items (CMDB records)	*TBD*	Refers to the number of CIs specifically. This doesn't take into account potential records representing relationships between CIs.

3.3.2 User Base Profile

3.3.2.1 SSC

The SSC user base for the Enterprise ITSM Tool Solution is summarized (by employee role) in the table that follows.

SSC Employee Role	Quantity	Description
Service Desk	80 Agents 10 Team Leads/Managers	SSC Enterprise Service Desk agents and management
Process Staff and Managers	580	SSC Staff supporting the ITIL Processes, such as Incident, Service Request, Change and Release Coordinators and managers, CAB, SACM.
Support Staff and Managers	2,800	Users utilizing the ITSM processes such as operational staff, Enterprise Command Centre (NOC), and service lines.
SSC Management	210	SSC Management will primarily use the Enterprise ITSM Tool to approve service requests and change requests, view dashboards and generate and consume reports. Any manager or above could be required to approve a service request or change request of some kind.
General Users	350,000	General users primarily interact with the self-service portal to initiate service requests, report incidents, check on the status of records they submitted, and access the knowledge base.
GC Customer Department Representatives	*TBD*	Representatives from Other Government Departments (OGDs) to log onto SSC's instance to check on the status of incidents, requests, BRs, change requests or CIs.

3.3.2.2 Pilot Department

The Pilot Department user base for the Enterprise ITSM Tool Solution is summarized (by employee role) in the table that follows.

Employee Role	Quantity	Description
Service Desk	*TBD*	Service Desk agents and management
Process Staff and Managers	*TBD*	Staff supporting the ITIL Processes, such as Incident, Service Request, Change and Release Coordinators and managers, CAB, SACM.
Support Staff and Managers	*TBD*	Users utilizing the ITSM processes such as operational staff, NOC, and service lines.
Departmental Management	*TBD*	Management will primarily use the Enterprise ITSM Tool to approve service requests and change requests, view dashboards and generate and consume reports. Any manager or above could be required to approve a service request or change request of some kind.
General Users	*TBD*	General users primarily interact with the self-service portal to initiate service requests, report incidents, check on the status of records they submitted, and access the knowledge base.

3.4 Collaborative Process for Configuration of ITSM Processes in the Enterprise ITSM Tool

3.4.1 Overview

The requirements implementation process will be collaborative, involving the ITSM Process Maturity Solution contractor and the Contractor, with oversight and support from SSC. Roles and responsibilities are identified in subsequent sections of this document.

The intent of the process is to deliver maximum value while supporting the following guiding principles:

- Remain flexible and adaptable at all times.
- High-value requirements will be prioritised higher than low-value requirements for implementation.
- Requirements will be accurately understood by all parties prior to implementation.
- All tool configurations and changes will be adequately documented and tested prior to release.
- Traceability will be maintained for all requirements, from requirement gathering through implementation to production

Through collaboration ITSM solution functionality will be delivered, as and when requested, through successive releases. The duration of each Release will be determined during the planning stage for each Release (maximum two weeks), and may differ from one another depending on the requirements being addressed at the time. For example, a relatively long release may be required for the initial implementation of an ITSM process, while shorter, iterative releases may be appropriate in the support of ongoing maturation of the process and tool in an incremental, valuable fashion.

3.4.2 Roles and Responsibilities

The ITSM processes will be developed, implemented collaboratively by SSC, the ITSM Process Maturity Solution contractor (PwC), and the Contractor, with high level responsibilities as follows.

Collaborative Process for Configuration of ITSM Processes in the Enterprise ITSM Tool Roles and Responsibilities	
SSC	• Contractor oversight of process onboarding onto Tool • Contractor management (including managing vendor inter-relationships) • ITSM Tool project management, including: o Project governance, including project reporting and integrated project schedule o Subject matter expertise related to SSC current processes, business requirements o Deliverable review and acceptance process o User acceptance testing (UAT) o Stakeholder management o Contract Management • Provisions and support of required hardware infrastructure in accordance with the EDC Services Technical Integration Information, provided as Appendix 6.
ITSM Process Maturity Solution Contractor	The ITSM Process Maturity Solution contractor has commenced work. Key activities and/or deliverables include: • Leveraging SSC requirements documentation, develop and document a detailed statement of business, functional and technical requirements for the ITSM Process Maturity Solution. • Document conceptually how each ITSM process will function within SSC and in relation to customer environments. • Perform a readiness assessment gap analysis for each of the ITSM processes against the capabilities of the selected Enterprise ITSM Tool (provided by the Contractor) as well as a gap analysis of the operational procedures to ensure SSC service commitments and customer business needs are met. • Perform business analyses of functional requirements to identify information, procedures, and decision flows for configuring the Enterprise ITSM Tool software. (**Note:** The ITSM processes to be designed must be configurable in the selected Enterprise ITSM Tool without customization as defined in section 10.6.1) • Develop and document detailed Functional Requirements for the ITSM Tool Solution.

Collaborative Process for Configuration of ITSM Processes in the Enterprise ITSM Tool Roles and Responsibilities	
	• Manage the requirements for the ITSM Tool Solution ensuring traceability. • Document an integrated deployment plan and checklist for each process transition to operational state and integrate with Contractor's cutover plan and checklist. • Organizational Change Management (OCM) program planning and execution to support the successful implementation of the new processes and Tool.
Contractor	The Contractor will supply, implement and support a complete ITSM Tool Solution including: • Enterprise ITSM Tool COTS software; • System integration professional services required to implement the new ITSM Tool solution; • System Testing; • Training Services; • Transition Services; • Application Management Services (AMS); and • Plan and execute data conversion. The requirements of the Contractor are more fully detailed in sections 4-16 of this SOW.

3.4.3 ITSM Process Design

The ITSM Process Maturity Solution contractor, in support of SSC's ITSM Process Evolution initiative, is responsible for the design of ten ITSM processes as listed in section 2.2.2. The ITSM Process Maturity Solution contractor will develop, prioritize and manage the ITSM functional requirements and deliver them to the Contractor for analysis and development of design specifications.

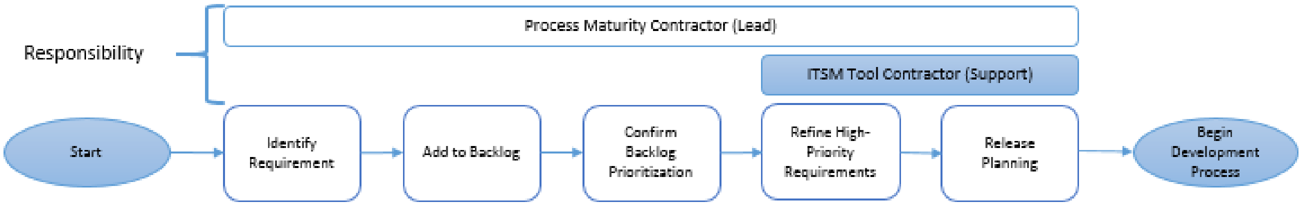
3.4.4 ITSM Process Requirements Management

The Requirements Management process for ITSM processes and associated tool functionality will be managed by the ITSM Process Maturity Solution contractor, supported by the Contractor.

Functional requirements will be recorded and managed in an ITSM Process Maturity Backlog. Owned and managed by the ITSM Process Maturity Solution contractor, the ITSM Process Maturity Backlog represents the cumulative list of desired ITSM process (and related) deliverables for the product and may include (but is not limited to) ITSM configuration and integration, report creation, enabling of features, bug fixes, documentation changes, and anything else that might be meaningful and valuable to the ITSM Process Evolution initiative.

The ITSM Process Maturity Backlog forms the basis of Release planning, by estimating the effort associated with the top priority backlog items and determining how many of the items will be delivered in the upcoming Release(s). It is possible that multiple project Releases will execute in parallel, representing different streams of ITSM Tool Solution implementation (E.g. ITSM Process configuration (various), reporting, integration, data migration).

The following diagram illustrates the envisioned ITSM Process Requirements Management process:


Responsibility
Process Maturity Contractor (Lead)
ITSM Tool Contractor (Support)
Start
Identify Requirement
Add to Backlog
Confirm Backlog Prioritization
Refine High-Priority Requirements
Release Planning
Begin Development Process

The responsibility to lead or support each step of the requirements process is further described in the following table:

ITSM Process Requirements Management Process	Responsibility		
	ITSM Process Maturity Solution contractor	**SSC**	**Contractor**
1. Identify Business Requirement	**Lead**	**Approve**	------
2. Add to Backlog	**Lead**	Support	------
3. Confirm Backlog Prioritisation	**Lead**	**Approve**	Support
4. Refine High-Priority Requirements	**Lead**	Support	Support
5. Tool Release Planning	Support	**Approve**	**Lead**

Each step of the development process is further described in the following table:

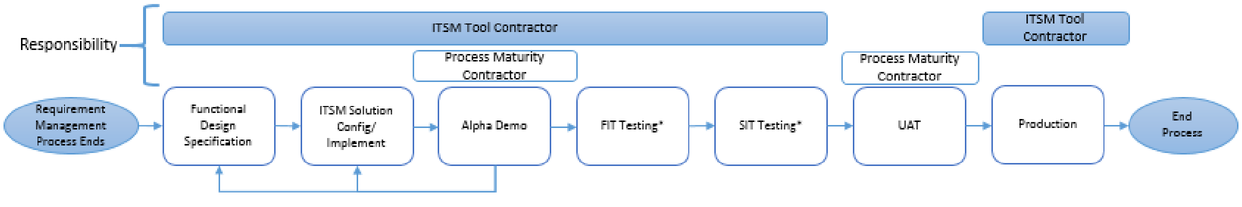
ITSM Process Requirements Management Process Steps	Description
1. Identify Business Requirement	Business requirements are continuously identified through process design and continual improvement initiatives.
2. Add to Backlog	New requirements are inserted into the process maturity backlog according to business priority.
3. Confirm Backlog Prioritisation	This is a regularly recurring activity during which the priority of the backlog items is reviewed to ensure they are listed in the correct order.
4. Refine High-Priority Requirements	The items near the top of the backlog are discussed in detail and broken into smaller requirements if necessary. At the end of this activity, each of the refined requirements has an associated functional requirement which is detailed enough for the Contractor to fully understand and provide effort estimates for configuration
5. Tool Release Planning	The high-priority items in the backlog are estimated in terms of effort and grouped logically into upcoming releases. The development process takes over at this time, for items assigned to an upcoming release.

3.4.5 Lifecycle for Configuration of ITSM Processes in the Enterprise ITSM Tool

The Contractor will lead a collaborative business systems analysis and tool configuration and development process that will involve representatives from SSC and the ITSM Process Maturity Solution contractor. The implementation process will take place in the context of one or more aforementioned releases.

Implementation of ITSM process requirements will be undertaken with responsibilities shared between the ITSM Process Maturity Solution contractor and the Contractor, in accordance with the process depicted below. All ITSM solution deliverables including, but not limited to ITSM process configuration, integrations, data migration, reports, and customization/coding will be developed following the same development process.

Note: Each Release will include a Planning period, of a maximum two weeks, during which time the scope of work and duration of each Release will be determined.


Responsibility
ITSM Tool Contractor
Process Maturity Contractor
Process Maturity Contractor
ITSM Tool Contractor
Requirement Management Process Ends
Functional Design Specification
ITSM Solution Config/ Implement
Alpha Demo
FIT Testing*
SIT Testing*
UAT
Production
End Process

* Testing processes are described in subsequent sections of this document

The responsibility to lead or support each step of the Tool configuration process is further described in the following table:

Tool Configuration Process	Responsibility		
	ITSM Process Maturity Solution contractor	**SSC**	**Contractor**
1. Functional Design Specification	Support	**Approve**	**Lead**
2. Configuration/ Development Phase	Support	Support	**Lead**
3. Alpha demo	Support	Support & **Approve**	**Lead**
4. FIT	Support	**-----**	**Lead**
5. SIT	Support	Support & **Approve**	**Lead**
6. UAT	Support	**Lead** & **Approve**	Support
7. Production	Support	**Lead** & **Approve** (provide Tier-1 support and trouble-shooting)	Apply changes to production & Provide Tier-2 support

Each step of the Tool configuration process is further described in the following table.

Tool Configuration Process Steps	Description
1. Functional Design Specification	The functional design specification is written. 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.).

Tool Configuration Process Steps	Description
	The functional design specification is reviewed with the ITSM Process Maturity contractor; this may be an iterative process for complex requirements. JAD sessions (Joint Application Design) may be used to expedite this step. SSC must accept the Functional Design Specification prior to configuration. The document is used as input for all downstream development process steps.
2. Configuration/Development Phase	The functional requirements are implemented in the ITSM Tool Solution according to the functional design specification. Unit testing is completed in this step.
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. The development process may return to Step 1 or Step 2 following an alpha demo.
4. FIT (Functional In-board Testing)	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
5. SIT (System Integration Testing)	System testing done in the test environment where application is run through a test suite to ensure that overall system functionality is not broken.
6. UAT (User Acceptance Testing)	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.
7. Production	The implementation of ITSM process functionality to production is primarily driven by the ITSM Process Evolution initiative, supported by the ITSM Process Maturity Solution contractor: - Planning - Organizational Change Management (OCM) o Training o Communications
	The Contractor manages the technical aspects of the implementation of new functionality in production environment: - Raises the necessary SSC change request(s) - Coordinating with other technical teams as required - Following SSC's change management processes - Communicating with identified stakeholders, change coordinators re: the status of the change

3.5 Project Organization

3.5.1 Project Governance

This project is a PCRA Level 3 project and it will be managed under the Project Steering Committee (ongoing issues, strategy/vision, and guidance) and the Project Management Board (gating approvals).

The project is being managed by the Project Management and Delivery Branch in support of the Transformation Program and will follow standard project governance processes required by SSC's Project Governance Framework (PGoF). As necessary, recommendations or requests from the Project Steering Committee are presented to other standard committees that are part of SSC's overall governance structure.

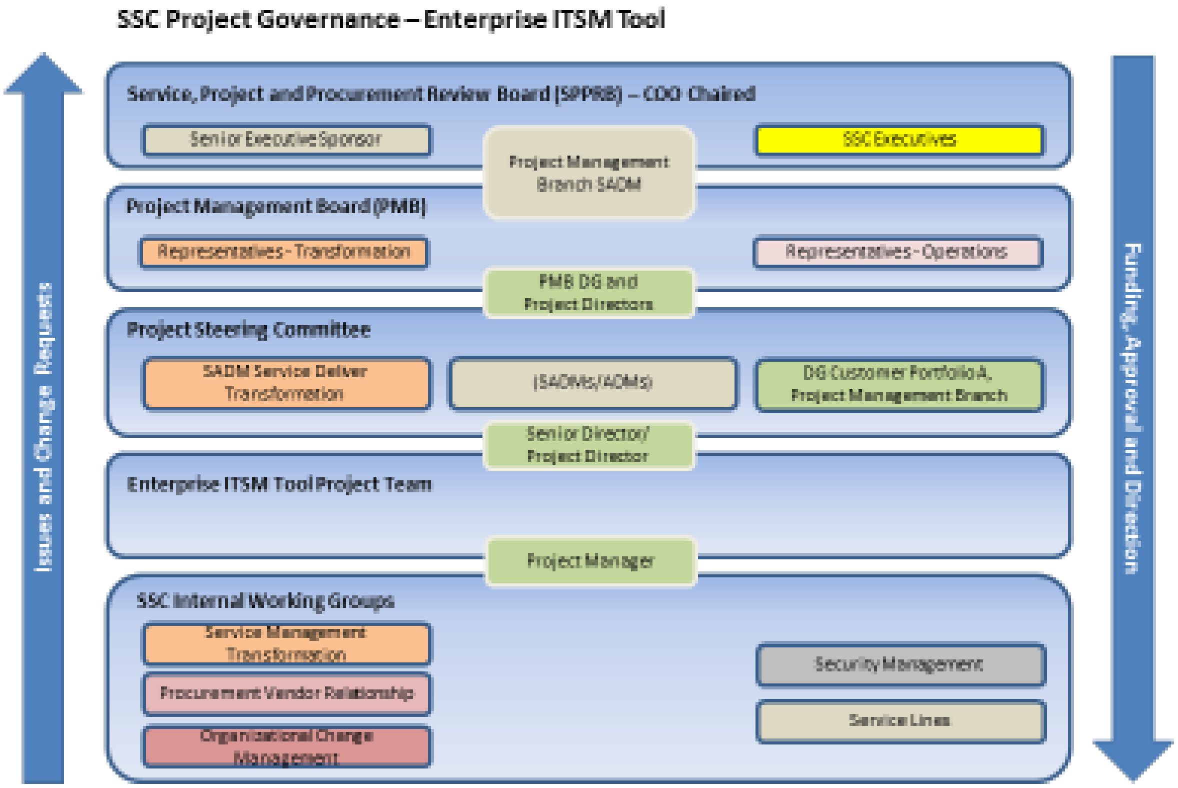

SSC Project Governance – Enterprise ITSM Tool
Service, Project and Procurement Review Board (SPPRB) – COO Chaired
Senior Executive Sponsor
Project Management Branch SADM
SSC Executives
Project Management Board (PMB)
Representatives - Transformation
Representatives - Operations
PMB DG and Project Directors
Project Steering Committee
SADM Service Deliver Transformation
(SADMs/ADMs)
DG Customer Portfolio A, Project Management Branch
Senior Director/ Project Director
Enterprise ITSM Tool Project Team
Project Manager
SSC Internal Working Groups
Service Management Transformation
Procurement Vendor Relationship
Organizational Change Management
Security Management
Service Lines
Issues and Change Requests
Funding, Approval and Direction

Figure 2: Enterprise ITSM Tool Project Governance

3.5.2 Enterprise ITSM Tool Project Roles and Responsibilities

Project Role	Responsibilities
Branch Head Sponsor	The Branch Head Sponsor is generally at the ADM level and is the executive accountable for realizing the benefits and business outcomes of the project. • Acts as champion for the project; • Approves the Business Case and other project deliverables prior to departmental review and approval; • Secures the required resources and funds to deliver the projects; • Stays abreast of project status; • Approves change requests (within authorized limits), or recommends to higher approval authority as required; • Reports on the realization of the benefits and project business outcomes.
Business Sponsor	The Business Sponsor is the person responsible for the business outcomes of the project, as well as providing the business requirements and the funding for the project. The Business Sponsor for SSC-led projects relating to services is the Service Lead. The Business Sponsor for new or changed internal SSC business processes or systems is the business owner of that process or system. The Business Sponsor for Customer-led projects is the Customer, however the Service Delivery Manager acts as “Internal Project Sponsor” on behalf of the Customer, for customer-led projects. • Defines the Business Case; • Facilitates the key organizational support needed to create a successful project; • Funds the project; • Accepts the results and outcome of the project, and will typically act as the business owner once the project’s deliverables are placed into operation; • Puts the service (i.e. the results of the project) into operation; • Provides business requirements, on behalf of the end users; • Coordinates the involvement of Customer representatives; • Provides validation, verification and testing of the project deliverables, including User Acceptance Testing; • Approves change requests (within authorized limits); and, • Ensures user adoption.
Project Steering Committee	Consisting of ADM and DG-level members, the key role of the Steering Committee is to provide guidance and oversight of the Process Evolution Initiative and Enterprise ITSM Tool Project. More specifically the Steering Committee ensures continuous alignment of project and initiative priorities and schedules, management of associated risks, and realization of benefits. The committee also serves as a governance and acceptance body of the ITSM Process Maturity Solution Contract deliverables, which is a key component of the ITSM Process Evolution Initiative. • Provide senior management direction, oversight and support to the project/initiative; • Review systemic project/initiative-related issues and associated resolution plans, including risk mitigation; • Ensure appropriate SSC stakeholders are involved in decision-making to ensure project/initiative objectives are met; • Ensure continuous alignment of the project/initiative with broader GC and SSC organizational plans and priorities;

Project Role	Responsibilities
	• Advocate timely completion of project/initiative deliverables and highlight consequences of change; • Through the co-chairs, direct the Committee with respect to major project/initiative decisions and artefacts; and • Through the co-chairs, discuss and escalate unresolved issues through SSC governance channels (PMB, SPPRB, etc.).
Senior Director / Project Director	The Project Management Executive is responsible for all projects and project managers in their directorate. • Operates a Project Management Office (PMO) for projects within the branch; • Ensures standards and best practices are adhered to; • Ensures that project data is up-to-date in the project repository tool; • Ensures that project deliverables are stored and kept current; • Ensures that project financial data is kept current in the financial system; • Liaises with the Project Management Centre of Excellence (PMCoE) for current templates, forms, best practices, and project oversight tools.
Project Manager	The SSC Project Manager (SSC PM) is fully responsible for the successful completion of the project including the day-to-day management of the project. The SSC PM's authority is set out in the Project Charter. The SSC PM reports to the Project Management Executive while being accountable to the Business Sponsor. The SSC PM: • Is fully responsible for the successful completion of the project; • Supports the Branch Head Sponsor and the Business Sponsor in the realization of the project outcomes; • Acts as the Technical Authority for the project; • Is responsible for day-to-day management of the project, including management of the Project Team; • Ensures adherence to the SSC Directive for Project Management; • Develops and secures approval for all project documents, such as the Project Charter and Project Management Plan; • Achieves the approved project scope within the planned (baseline) cost and schedule; • Monitors variances in the project scope, cost and schedule against the approved scope, cost and schedule baseline plans, and takes required corrective actions; • Implements communications plans, and ensures engagement of stakeholders; • Ensures proactive and continuous management of risks and issues, facilitating the resolution or appropriate escalation; • Ensures Project Change Requests for all changes to baseline scope, cost and schedule are completed and approved; • Provides timely, consistent, and accurate project status reporting.

4 OVERVIEW OF ITSM TOOL CONTRACTOR REQUIREMENTS

The work to be delivered under this Contract includes:

	Reference
a) Contractor Management and Oversight Services	SOW 5
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 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.	SOW 6
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 Pilot Department; and b. Additional capacity to support on-boarding of customers to the ITSM Tool Solution.	SOW 7
d) 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. Technical Training of the SSC Project Team; 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).	SOW 8 to 14
e) Transition Services, including: a. Develop Transition plan; b. Conduct knowledge transfer activities; and c. Transfer responsibility for management and operation of ITSM solution to SSC.	SOW 15
f) Provision of Application Management Services (AMS), including: a. AMS for a one year following implementation (including HyperCare period); and b. (Optional) AMS for up to five additional 1-year option periods.	SOW 16

5 CONTRACTOR MANAGEMENT AND OVERSIGHT SERVICE REQUIREMENTS

5.1 Contractor Governance

The Contractor must utilize a formally documented governance model to manage its Work. The Contractor governance model must work in conjunction with, and be complementary to, the SSC ITSM Project Governance Structure set out in section 3.5.1 above. 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 ITSM Project Executive Sponsor. This role is to be fulfilled at no direct cost to Canada 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 Technical Authority and the primary interface with the ITSM Process Maturity contractor. The Contractor PM must support ITSM 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 Enterprise ITSM Tool Software Publisher must designate a Representative to participate as a member of the Contractor's Governance Team and 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 Enterprise ITSM Tool COTS Software product and its future direction as well as identify technical experts from the Enterprise ITSM Tool Software Publisher that may be required to the support the Enterprise ITSM Tool Project.

5.2 Project Management and Oversight

a) The Contractor 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.

b) The Contractor must apply project management discipline in accordance with industry standards as well as align to the SSC Project Governance Framework (PGoF) to ensure that 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.

c) The Contractor PM is responsible and accountable for project delivery of the ITSM Tool Solution and will provide project 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 progress of the ITSM Tool Solution deliverables.)

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

e) The Contractor must implement, maintain and use the Contractor Work Plan (CWP) 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.

5.3 Contractor’s Core Delivery Team

a) The Contractor must establish a Core Delivery Team (hereafter referred to as the Core Team), led by a dedicated Contractor Project Manager (as stipulated in SOW 5.1).

b) The Contractor’s Core 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 other professional services resources, expertise and guidance to the Contractor’s delivery team as necessary during the performance of each specific Deliverable under the Contractor Management and Oversight Services set out in SOW article 5.2.

c) The composition of the Core 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 under the Contract, but at a minimum must include the following:

   a. A Contractor Project Manager (PM) 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 36 months. (Note: 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. Additional (full-time or part-time) resources (e.g. Project Coordinator resource, etc.) the Contractor deems necessary to support the Contractor’s Project Management Team function as set out in section 5.2 above.

   c. Resources designated 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
      ii. Integration Specialist

d) During the period of the Contract, the Contractor may augment its’ Core Team with the additional resources and expertise it deems necessary to complete specific Deliverables under the Contract in accordance with the CWP.

5.4 Location of Work

a) SSC will provide office accommodations for up to eight members of the Contractor’s Work Team on-site at a GC location in the NCR location including:

- Workspaces comprised of work surfaces, storage pedestal and chair, sized according to Government of Canada 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.

b) The Contractor may, at its discretion, conduct ITSM Tool configuration work off-site at its own location in Canada, using its own development processes and tools. The Contractor is responsible for bringing deliverables which are developed off-site into the SSC environment. When the work is conducted off-site, the resources must be fully contactable during all working hours, and available to meet onsite at SSC upon request.

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

d) Application Management Services, as set out in SOW section 16, must be delivered from the Contractor's Canadian Operations Centre location.

5.5 Contractor Work Plan and Schedule

a) During the delivery of the Contractor Onboarding activities set out in SOW section 8, the Contractor PM must update the proposed Contractor Work Plan and Schedule (CWP&S) (contained in the Contractor's Bid) 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.

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 for inclusion in the integrated Enterprise ITSM Tool Project plan and schedule. 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 8.

f) The SSC PM will incorporate the CWP&S into the integrated Enterprise ITSM Tool Project plan and schedule.

5.6 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; and
n. 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 on SSC (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) Canada 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.

5.7 Monthly Progress Report

The Contractor must prepare and deliver a Monthly Progress Report which describes the status of the contract's activities, deliverables and timetable, which are used to update the CWP and CS. This report must be submitted to the SSC PM within two weeks 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)
2.2. Phase
2.3. % Completed
2.4. Plan Start
2.5. Plan Complete
2.6. Actual Start

3. Progress Report Summary
3.1. Key Project Deliverable

3.2. Status
3.3. Planned Completion Date
3.4. Revised Completion Date 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

5.8 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.

b) The QM Plan will be delivered as part of Contractor Onboarding as set out in section 8 of this SOW. 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 proceed with Work until the SSC PM has approved the QM plan.

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

d) The Contractor must manage the Contract in accordance with the accepted QM plan.

5.9 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 8 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 Contract in accordance with the accepted Risk Management Plan and the terms and conditions of this Contract.

5.10 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 8 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.

5.11 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.

5.12 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. All PS resources must meet the mandatory requirements associated with the applicable resource category as identified in Appendix 3, Resource Assessment Criteria.

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

Experience Level	Years of Experience in the Role
Senior	Over ten years
Intermediate	Five to ten years
Junior	Less than five years

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

5.12.1 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.

5.12.2 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.

5.12.3 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.

5.12.4 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 Canada 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.

5.12.5 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.

5.12.6 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.

5.12.7 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.

5.12.8 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.

5.12.9 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.

5.12.10 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.

5.12.11 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.

5.12.12 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.

5.12.13 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;
e) Use document management software to perform work;

5.12.14 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.
e) Work with importing files from heterogeneous platforms.

5.12.15 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.

5.12.16 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.

5.12.17 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.

5.12.18 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.

5.12.19 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.

6 ENTERPRISE ITSM TOOL REQUIREMENTS

6.1 Contractor Requirements

a) The Contractor must provide an Enterprise ITSM Tool (i.e. Licensed Software).

b) The Enterprise ITSM Tool must be a single technological architecture (i.e. single suite of software) from a single Software Publisher.

c) The Enterprise ITSM Tool provided by the Contractor must meet each of the Non-Functional Requirements set out in Appendix 1 to this SOW.

d) The Enterprise ITSM Tool provided by the Contractor must deliver ITIL standard processes and functionality listed below and meet the Functional Requirements set out in Appendix 2 to this SOW:

e) The ITSM Tool provided by the Contractor must include sufficient licenses to support the estimated number of end-users (by user category) as set out in section 3.3 above.

f) The Contractor must provide documentation for the Licensed Software, in accordance with the supplemental General Conditions 4003, as set out in Part 7 – Resulting Contract Clauses.

g) The Contractor must provide Software Maintenance and Support for the Licensed Software, in accordance with the supplemental General Conditions 4004, as set out in Part 7 – Resulting Contract Clauses, including:

   a. Software Error Correction Services
   b. Maintenance Releases
   c. Media
   d. Support Services
   e. On-site Services

h) The Contractor must provide Software Upgrades for major releases of the Enterprise ITSM Tool to maintain current to version *n*-1 for the period of the contract, including option periods.

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

7 HARDWARE SPECIFICATION REQUIREMENTS

7.1 Identification of Hardware Specifications

a) The Contractor must provide SSC with the specification for the hardware infrastructure to be provided by SSC, including the following environments:

  a. Development environment;

  b. Testing environment;

  c. Production environment;

  d. Training environment;

  e. Reporting environment; and

  f. Disaster Recovery environment.

b) The infrastructure specifications must include all required hardware and middleware to make the system work including switching to a disaster recovery site with data current to one (1) day.

c) The infrastructure specifications must include hardware for storage for attachments and system log files, etc.

d) The specifications for initial hardware infrastructure must be of adequate capacity to support the estimated minimum number of Users and Volumetric Data (for SSC and the Pilot department) as set out in sections 3.3 above.

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 provide the specifications to SSC and provide a minimum of a 14-week window to allow SSC to procure and install any required infrastructure.

8 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 infrastructure necessary to commence the Work associated with the Functional Design and Configuration of the Enterprise ITSM Tool. The Contractor Onboarding activities **must be completed within 90 days of Contract Award** and must include, at a minimum, the following deliverables:

8.1.1 Deliverable #1: Review and provide input to SSC ITSM Process Maturity Solution draft documents

a) Within 5 days of Contract Award, SSC contemplates providing the Contractor with Enterprise ITSM Tool Project plans and ITSM Process Maturity Solution contactor deliverables. The Contractor must review and, where applicable, provide input to these documents. These include, but are not limited to, the following documents:
   - i. Functional Requirements
   - ii. OCM Strategy and Plan
   - iii. Latest version of the ITSM Process Maturity Backlog (including User Stories)
   - iv. 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 days of Contract Award, the Contractor must participate in a Contractor Solution Impact Meeting with the SSC PM and key members of the Project Team. The purpose of the meeting is for the Contractor to:

   i. Identify any information contained in the a Enterprise ITSM Tool Project plans and ITSM Process Maturity Solution contactor deliverables documents provided by SSC (listed 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.

8.1.2 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 5.1 above), 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 5.3 above), introducing the key resources and their roles and responsibilities and how they will work with SSC's Project Team; and
c) Onboarding initial Contractor resources will take place once the Contractor Core Delivery Team plan is accepted by SSC's Project Team.

8.1.3 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 SOW section 5.8 above.

8.1.4 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 SOW section 5.9 above.

8.1.5 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 SOW section 5.10 above.

8.1.6 Deliverable #6: Release Management Strategy

The Contractor must develop a Release Management Strategy for SSC acceptance. The Release Management Strategy must support the Collaborative Process for ITSM Process Design and Tool Configuration in section 3.4, and the ITSM Tool Implementation requirements in section 10. The Contractor is required to deliver a Release of the ITSM Tool once per Fiscal Quarter, at a minimum.

8.1.7 Deliverable #7: Updated CWP&S

a) The Contractor must update and finalize the Contractor Work Plan and Schedule (CWP&S) proposed in the Contractor's Bid (see section 5.5 above). The CWP&S must be updated to reflect Contract award dates, 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 required Work and clearly identify the tasks, milestones, deliverables, interdependencies and critical path.

b) The updated 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.

9 DATA MIGRATION REQUIREMENTS

9.1 Scope and 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.

SSC anticipates that data migration and/or data creation activities required to the new system will 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 ITSM tool. (Note: There are over 15,000 user accounts in ECD the legacy tool, however there are only 4,000 staff in SSC, 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 ITSM 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.

9.2 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:

9.2.1 Data Migration Plan

The Contractor must 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. The Data Migration Plan must be completed and submitted within 30 days of the completion of Contactor Onboarding (set out in section 8). 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.

9.2.2 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 Enterprise ITSM Tool;

d) Reconcile the migrated data in the Enterprise 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 Enterprise ITSM Tool;

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

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

i) Provide support for user acceptance.

10 ITSM TOOL IMPLEMENTATION REQUIREMENTS

10.1 Overview

The Contractor is responsible for the configuration activities associated with all functional, non-functional, security and integration requirements identified in this SOW and its appendices.

The Contractor will lead the Tool Implementation Work, to be conducted in releases which may vary in duration depending on the scope of the release. The work to be conducted by the Contractor includes:

- ITSM Tool Release Planning and Management
- 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

Note: The same activities and deliverables are associated with each release.

The ITSM Tool Solution, including the Contractor's ITSM Tool Implementation deliverables, must meet the non-functional requirements set out in Appendix 1 to this SOW.

10.2 ITSM Process Implementation

The Contractor must work collaboratively with SSC and the ITSM Procuress Maturity Solutions Contractor, as described in section 3.4 above, to implement ITSM process requirements.

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 Enterprise ITSM Tool Solution within the cost and schedule parameters agreed with the SSC Technical Authority.

10.3 ITSM Tool Release Planning and Management

The Contractor must develop and maintain an ITSM Tool Roadmap (i.e. Release Management Pan) 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 is responsible for 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 the SSC ITSM Process Evolution initiative in conjunction with the ITSM Process Maturity Solution contractor.

Releases should 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.

10.4 Consultation with SSC and ITSM Process Evolution Stakeholders

The Contractor is responsible for consulting 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 the ITSM Process Maturity Solution contractor (described in section 3.4).

10.5 Development of Design Specifications

The Contractor is responsible for producing Design Specifications for all implementation or configuration activities. Design specifications should be traced back to the corresponding requirements. 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, the detailed functional requirements will be developed by the ITSM Process Maturity Solution contractor.

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

10.6 Configuration of the Tool

All changes to the ITSM Tool are required to follow the Software Development Lifecycle identified in section 10.8.1 below.

10.6.1 Configuration

10.6.1.1 Definition

SSC’s intends to address its ITSM Tool functional requirements by leveraging configuration settings that are available in the COTS ITSM Tool software rather than customizing the software. For the purposes of this contract, to be deemed configuration of the ITSM, the resulting feature, business rule or workflow:

1. 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
2. Must not require coding or knowledge of any industry or proprietary coding or scripting language.

3. Must not involve modifications or overlays of objects or components originally shipped with the product.
4. Must be supported by the Software Publisher's standard Maintenance and Support Services for the Licensed Software.
5. 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.

10.6.1.2 Changes to the Tool

In cases where requirements are unable to be met to SSC's satisfaction through configuration (as defined above), the Contractor must propose alternative solution(s) to SSC prior to proceeding, along with any associated costs, risks, dependencies and impacts to schedule of each alternative.

10.6.2 Contractor Configuration Requirements

10.6.2.1 Configuration Activities and Deliverables

The Contractor must configure (for each Sprint) the Enterprise ITSM Tool including but not limited to the following activities and deliverables:

a) Develop the detailed solution and user experience (UX) designs for each Sprint;

b) Develop the system security controls for each Sprint;

c) Configure each Sprint;

d) 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; and

e) Test (Unit, SIT, Performance/Stress, UAT support).

10.6.2.2 Integration Configuration

The Contractor is required to implement the integrations as identified in section 11, Integration Requirements.

10.6.2.3 Configuration Recommendations and Advice

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

10.7 Testing

For any given release, the Contractor must conduct all necessary testing to ensure the release will pass subsequent acceptance tests at SSC. Refer to section 12 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 8).

After the Contractor has verified successful migration, SSC resources will perform acceptance tests of the released solution. Any errors identified during the acceptance testing must be corrected by the Contractor at no additional cost to Canada in accordance with the Deliverable Review and Acceptance Process (to be agreed to by Canada and the Contractor) described in section 8 herein. The final such release will indicate readiness to release to the SSC production environment.

10.8 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.

10.8.1 Software Development Lifecycle (SDLC)

The contractor is required to 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 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.

10.8.2 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.

10.8.3 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.

10.8.4 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

11 INTEGRATION REQUIREMENTS

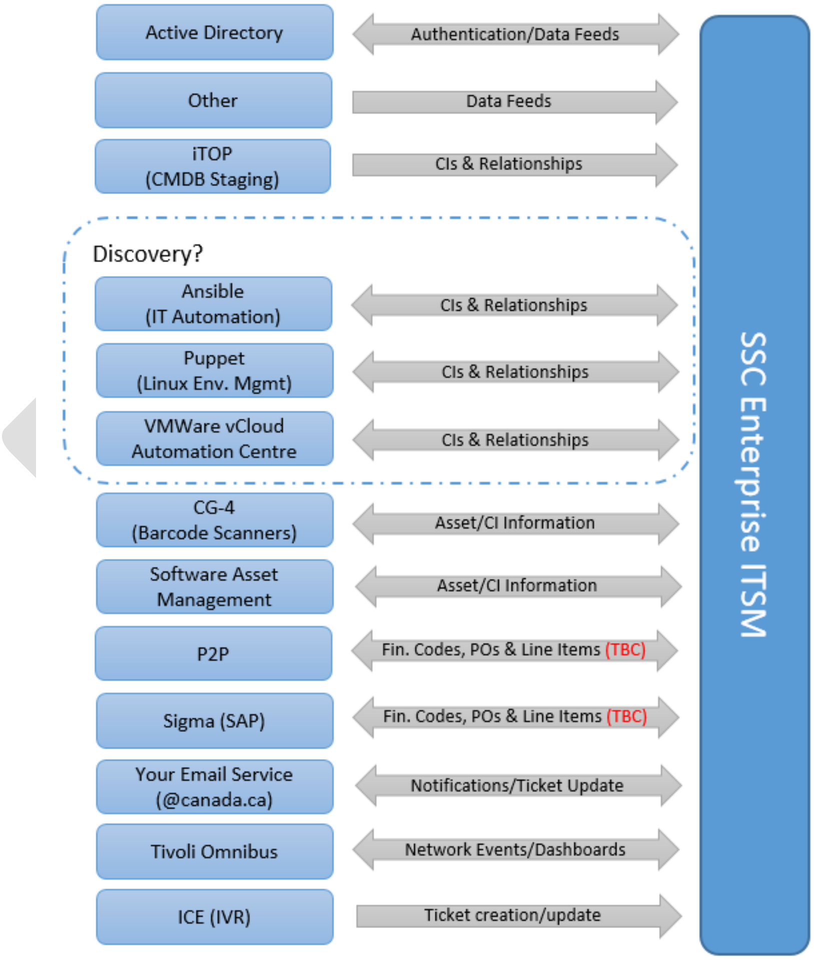
11.1 General Integration Requirements

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.

11.2 Integration with SSC Applications

Integrations between the ITSM Technical Solution and other SSC and GC applications are required to be delivered by the Contractor. The following diagram illustrates the scope of integrations with other SSC applications. For each integration, SSC will provide access to the relevant subject matter experts.



11.2.1 Directory Services (Active Directory)

The ITSM Technology Solution must deliver the capability to authenticate ITSM users of all types using SSC's Enterprise Directory Services solution. The Contractor is responsible for identifying to SSC use cases or situations where this is not possible, and propose alternative solutions.

11.2.2 Organizational Data Feeds

The ITSM Technology Solution must automate the loading of foundational data that supports tool functionality. For example (but not limited to):

- Employees and related data
- SSC and government locations and addresses

11.2.3 iTOP (CMDB Staging)

SSC is in the process of deploying iTOP to collect CMDB data from GC Customer departments, and run extract, transform and load (ETL) processes to prepare the data to load into SSC's legacy CMDB. The ITSM Technology Solution being implemented by this project is required to support and accept data from this process.

11.2.4 Ansible

SSC requires that servers and infrastructure being managed in SSC's Ansible environment are automatically represented as CIs in the ITSM Technology Solution's CMDB along with all relevant relationships. Ansible is an IT automation engine that automates cloud provisioning, configuration management, application deployment, intra-service orchestration, and many other IT needs.

11.2.5 Puppet

SSC requires that servers and infrastructure being managed in SSC's Puppet environment are automatically represented as CIs in the ITSM Technology Solution's CMDB along with all relevant relationships.

11.2.6 VMware vCloud Automation Centre (VCAC)

SSC requires virtual servers and infrastructure that are instantiated in SSC's VCAC environment are automatically represented as CIs in the ITSM Technology Solution's CMDB along with all relevant relationships.

11.2.7 CG-4

CG4 is an asset tracking system currently in use at SSC, and must be integrated with the ITSM Technology Solution to support bi-directional exchange of asset information.

11.2.8 Software Asset Management

<<details to be provided in final RFP>>

11.2.9 P2P

<<details to be provided in final RFP>>

11.2.10 SIGMA (SAP)

<<details to be provided in final RFP>>

11.2.11 "mailto:YourEmail@Canada.ca" (Enterprise Email)

The ITSM Tool must use SSC's "Your Email Service" (YES) @canada.ca enterprise email solution for:

- Outgoing ITSM notifications
- Incident and/or request creation and updates via inbound email messages.

The ITSM solution must support the following requirements:

- TLS over port 587
- Access to email system through a service account with credentials (no anonymous access will be permitted)
- The ITSM solution must not spoof the <From> address in outbound emails. For example, the ITSM solution must not substitute the service account with the account of an ITSM user who may have triggered the notification.

11.2.12 Tivoli Omnibus

Omnibus is used in multiple locations of SSC's Enterprise Command Centre (ECC) to monitor network events originating from various GC monitoring tools.

11.2.12.1 Event Management – Incident Creation and Update

ECC staff require the ability to create an ITSM incident directly from the Omnibus console(s), passing relevant data to the incident.

11.2.12.2 iESP Dashboards – Incident Update

The ECC has developed a series of iESP dashboards in Omnibus to provide different views of events for various Customer departments, or portfolios of Customer departments. ECC staff require the ability to update the work log of associated ITSM incidents. The Omnibus dashboards need to reflect the pertinent information entered on ITSM incident, and this must happen in real time.

11.2.13 ICE (IVR)

<<details to be provided in final RFP>>

11.3 Interoperability with GC Customer ITSM tools

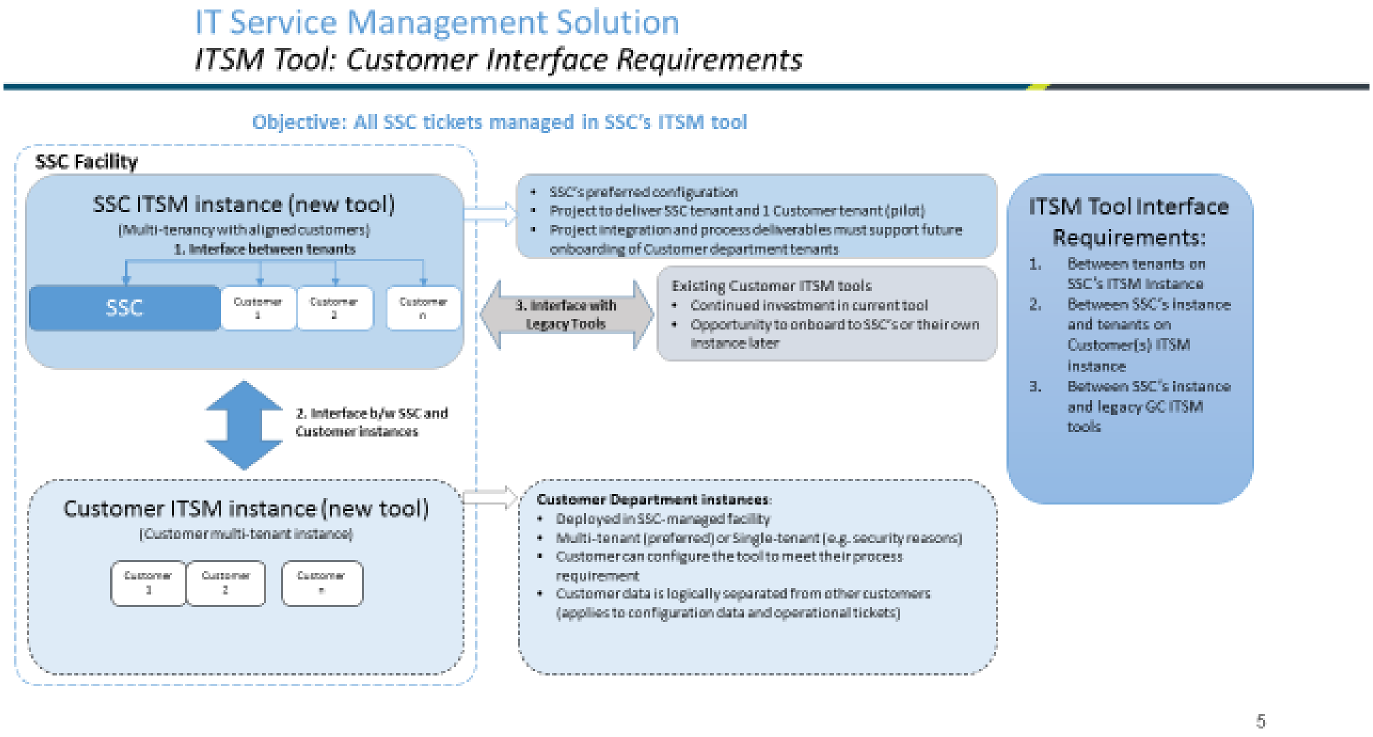
11.3.1 Bi-directional Interface Requirements

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 following diagram illustrates the integration scenarios that 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 Enterprise ITSM Tool 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.



IT Service Management Solution

ITSM Tool: Customer Interface Requirements

Objective: All SSC tickets managed in SSC's ITSM tool

- SSC's preferred configuration
- Project to deliver SSC tenant and 1 Customer tenant (pilot)
- Project integration and process deliverables must support future onboarding of Customer department tenants

Existing Customer ITSM tools
- Continued investment in current tool
- Opportunity to onboard to SSC's or their own instance later

Customer Department instances:
- Deployed in SSC-managed facility
- Multi-tenant (preferred) or Single-tenant (e.g. security reasons)
- Customer can configure the tool to meet their process requirement
- Customer data is logically separated from other customers (applies to configuration data and operational tickets)

ITSM Tool Interface Requirements:
1. Between tenants on SSC's ITSM Instance
2. Between SSC's instance and tenants on Customer(s) ITSM instance
3. Between SSC's instance and legacy GC ITSM tools

SSC Facility
SSC ITSM instance (new tool)
(Multi-tenancy with aligned customers)
1. Interface between tenants
SSC
Customer 1
Customer 2
Customer n
3. Interface with Legacy Tools
2. Interface b/w SSC and Customer instances
Customer ITSM instance (new tool)
(Customer multi-tenant instance)
Customer 1
Customer 2
Customer n
5

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. ITSM Process Uses Cases Examples are contained in Appendix 8.
- Support updates to a single record or multiple records in a single transaction.

11.3.2 Transactional Requirements

The ITSM Integration Solution must support:

a) the ITSM process descriptions, workflows, and data statements for the Request Fulfillment, Incident Management, Change Management and Service Asset and Configuration Management processes; and

b) the interactions between SSC and customer department/agency ITSM tools and processes.

11.4 Discovery

The ITSM Tool Solution provided by the Contractor must include the capability to discover assets in SSC's data centres. The Discovery solution must meet the following requirements:

- The Discovery solution must be agentless, requiring no installation of agents or other software in order for a given asset to be discovered.
- The Discovery solution must be able to discover infrastructure managed in VMWare vCenter.
- The Discovery solution must be able to identify (and recognize) commercially available infrastructure assets and applications. This feature must be available upon installation and require no additional configuration.
- The Discovery solution must recognize and identify dependencies between infrastructure assets, and applications.
- The Discovery solution must provide a visual user interface that allows Discovery administrators to model applications, services, and infrastructure.
- The data gathered by the Discovery solution must support the functionality contained in ITSM Tool.
- Discovery and/or ITSM administrators must have full control over which of the data gathered by the Discovery solution is made available to the ITSM Tool.

12 SYSTEM TESTING REQUIREMENTS

12.1 Contractor Testing Requirements

The Contractor must participate in the various types of ITSM solution testing in accordance with the type of testing, roles and responsibilities identified in section 3.4 above. 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

12.2 Unit Testing

The Contractor must conduct unit testing for any coded or configured deliverables prior to releasing for FIT testing.

12.2.1 FIT Testing (Functional In-board Testing)

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

12.2.2 SIT Testing (System Integration Testing)

The Contractor must define, implement and coordinate the SIT testing process.

12.2.3 UAT (User Acceptance Testing)

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

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 GC working days.

c) In the event that SSC discovers an issue, SSC will provide feedback to the Contractor within 15 GC working 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 GC working days to implement that process into the production environment.

13 TRAINING SERVICES REQUIREMENTS

13.1 ITSM Tool Orientation Session

The Contractor must prepare and conduct an ITSM Tool Orientation Session that will provide ITSM Process Evolution initiative stakeholders (including the ITSM Process Maturity Solution contractor) 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 session may have to be delivered on multiple occasions.

Attendees must complete the ITSM Tool Orientation session 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 Session must be classroom-based in the National Capital Region (NCR - Ottawa and Gatineau), and the Contractor must provide all course materials which can be retained by attendees for future reference.

13.2 Process Administrator Training

The Contractor must prepare and conduct training for SSC stakeholders who have been nominated to take on process administrative responsibilities. This training must be classroom based and available on an ad-hoc basis with agreed notice. The content of each training course will be negotiated in advance, but must be able to cover any of the process configuration topics that are appropriate to be done by business analysts and don't 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.

13.3 Train-the-Trainer

The Organizational Change Management (OCM) organization under SSC's Service Management Transformation is responsible for providing integrated ITSM tool and process training to all categories of end users at SSC and the Pilot customer department.

The Contractor must prepare and conduct "train the trainer" training courses to OCM trainers so that they have the necessary tool knowledge which they can incorporated into their integrated tool/process training to end users. The Contractor must provide the necessary training material and user manuals to OCM in order to support their training initiative.

The Train-the-Trainer course must be delivered multiple times, on demand, with an agreed period of notice.

13.4 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.

13.5 Required Training Materials

a) The Contractor must provide the Technical Authority with the following information for review and acceptance no less than 7 calendar days prior to the start of any training course:

   a. a course syllabus;

   b. a course schedule; and

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

b) 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.

c) SSC will provide either its approval or any comments it has regarding the above materials within ten GC working days. The Contractor must address those comments before using the materials for training.

14 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 SSC customer departments/agencies to onboard to SSC's instance of the Enterprise ITSM Tool 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 5.12 and the Resource Assessment Criteria contained in Appendix 3.

15 TRANSITION OUT SERVICES REQUIREMENTS

The Contractor must support the Enterprise ITSM Tool application, as set out in section 16. SSC, at its option, will transition responsibility for management of the Enterprise 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 Enterprise ITSM Tool Solution including, but not limited to, configuration of the tool and application management and operations.

Transition Out requirements are more fully described below.

15.1 Transition Plan

The Contractor must 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 Transition Plan must incorporate, but is not limited to, the following topics as outlined in the following sections.

15.1.1 Resource Plan

The Contractor 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 organization structure and Government of Canada HR policies and should include all roles involved with the ITSM Tool Solution and their respective responsibilities and accountabilities.

15.1.2 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. Delivery of any courses or issuing of certification may be provided by the Contractor, or a 3rd party if necessary.

15.1.3 Knowledge Transfer Plan

The Transition Plan must include a register of all required knowledge transfer topics, which SSC stakeholders need to attend, and propose a schedule for conducting knowledge transfer sessions with the identified recipients of the knowledge transfer.

15.1.4 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 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 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.

15.1.5 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.

15.1.6 ITSM Software Support Channels

The Contractor must establish and provide SSC with the mechanisms and procedures to contact the ITSM Tool manufacturer (or Contractor, if appropriate) in order to report incidents, download ITSM software patches and new versions, download ITSM product manuals, and access the ITSM manufacturers support website.

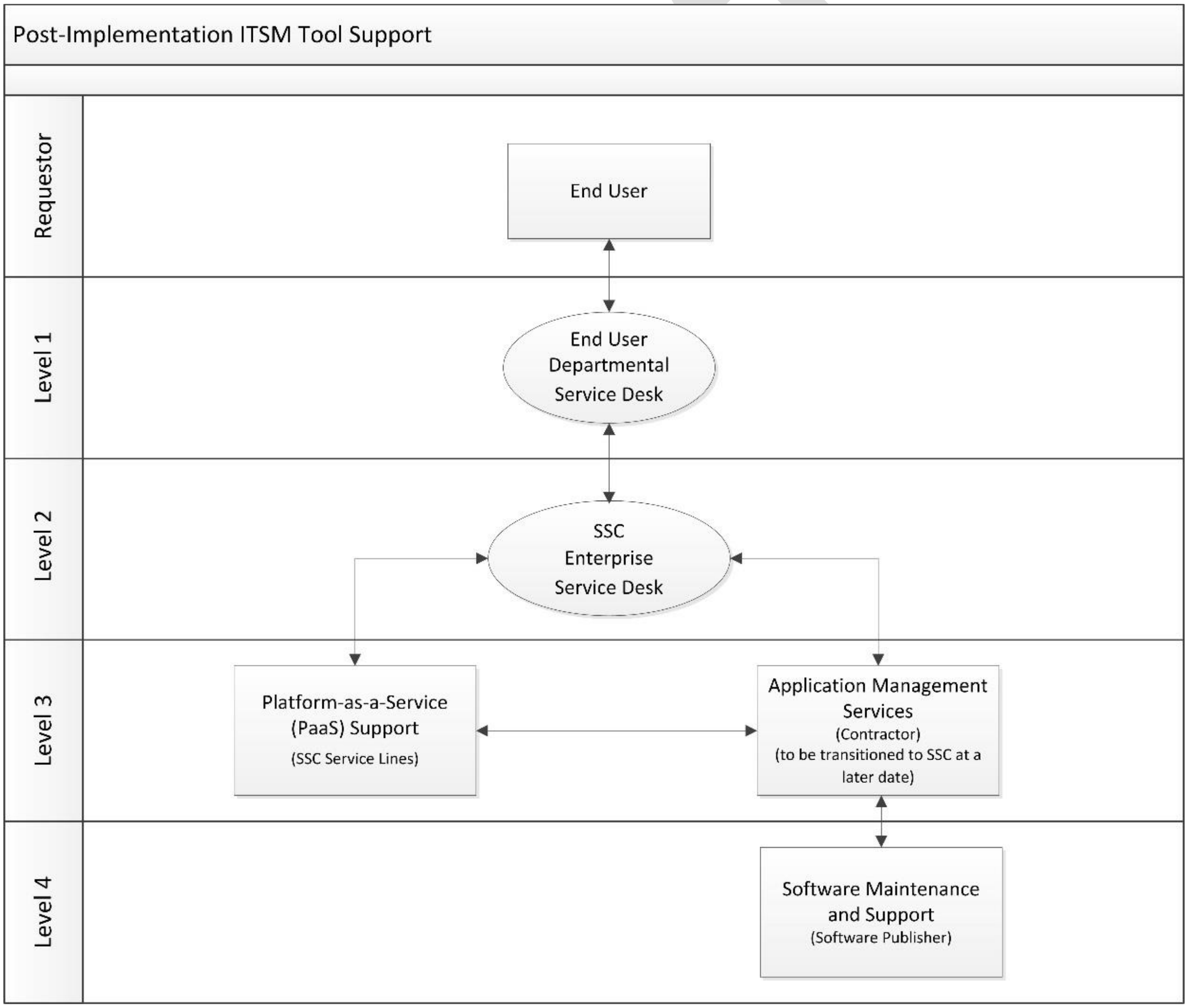
15.2 Execution of Transition Plan

The Contractor must execute the approved Transition Plan as and when requested by SSC.

16 APPLICATION MANAGEMENT SUPPORT

16.1 Post-Implementation Support Model

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


Post-Implementation ITSM Tool Support
Requestor
Level 1
Level 2
Level 3
Level 4
End User
End User Departmental Service Desk
SSC Enterprise Service Desk
Platform-as-a-Service (PaaS) Support (SSC Service Lines)
Application Management Services (Contractor) (to be transitioned to SSC at a later date)
Software Maintenance and Support (Software Publisher)

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

  ITSM End-users submitting requests related to the Enterprise ITSM Solution or experiencing issues with the solution 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 Enterprise ITSM Solution, the departmental service desk will escalate the incident or request to 2nd level support: SSC's Enterprise Service Desk.

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

  Upon receipt of an Enterprise ITSM 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.

- **<u>3rd Level Support</u>**
  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.

- **<u>4th Level Support</u>**
  4th level support for ITSM Tool application related incidents will be provided by the ITSM Tool Software Publisher.

16.2 Hypercare Support Services

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

Hypercare support services are the increased levels of support services, over and above routine AMS operational support levels, necessary to manage the typical increase in system Incidents and customer support calls immediately following production implementation of a new release.

For the Initial Release of the Enterprise ITSM Tool Solution, Hypercare Support Services must be provided 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 Severity 1 Incidents being raised during month-end processing;
2) All data migrations have been completed;
3) All system interfaces to and from the Enterprise ITSM Tool Solution have completed a pre-determined representative sample of processing in production at least once without any Severity 1 or Severity 2 Incidents;
4) There are no open Severity 1 or Severity 2 Incidents related to the Release;

5) The “Measuring Impact - Post- implementation evaluation and remediation” activities and Deliverables must be completed; and
6) The following Service Level Requirements (SLRs) have been met for at least one month:
    a. SLR 1.4-1 Application Performance Response Time;
    b. SLR 1.4-2 Application Availability;
    c. SLR 1.4-4 Incident Response Time; and
    d. SLR 1.4-5 Incident Resolution Time.

Note: Refer to Draft Contract Terms (of this RFI) for details of the SLRs, including definitions of Severity levels.

The Contractor must provide Hypercare Support Services for all subsequent Releases of the Solution for the duration of the Contract. All SLRs (as set out in the Draft Contract Terms of this RFI) must continue to be met throughout all Hypercare support periods for all subsequent Releases unless exclusions or modifications to the SLRs for the period of the Hypercare Support Services are pre-approved in writing by the Technical Authority prior to implementation of the Release. Hypercare Support Services must be performed until such time that the above conditions have been met.

16.3 Application Management Support Service Requirements

16.3.1 Application Management Services

a) 3rd Level Application Management Services, relating to the Enterprise ITSM 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 Enterprise ITSM Solution:

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

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

    c. Record, within the Enterprise 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 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 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 Enterprise ITSM Solution are required, in accordance with SSC processes, policies and procedures for Change Management;

    h. Create and maintain a model of the Enterprise ITSM Solution in the Enterprise ITSM Solution’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 application, 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 lesson-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 application related components (ITSM Tool, database, middleware);

n. ITSM database administration and support;

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

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

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

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

s. Create and maintain an ITSM Solution knowledge database, including lessons learned over the duration of the contract, within the Enterprise 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 Enterprise ITSM 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 solution implementation for SSC.

c) The Service Level Requirements, and associated remedies, for AMS are stipulated in the Draft Contract Terms (of this RFI).

16.3.2 AMS Requirements

a) The Contractor must provide 3rd Level AMS services (as per 16.3.1) 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 15 above) in order to transition responsibility for AMS from the Contractor to SSC's application management support team.

16.3.3 Optional to extend AMS

a) The Contractor must, if and when requested, provide 3rd Level AMS services (as per 16.3.1) for up to five additional one- year periods.

b) The Contractor must, if and when requested, conduct Transition activities (as set out in section 15 above) in order to transition responsibility for AMS from the Contractor to SSC's application management support team.

APPENDIX 1 – ITSM TOOL NON-FUNCTIONAL REQUIREMENTS

The Enterprise ITSM Tool software provided by the Contractor must meet each of the Non-Functional Requirements stipulated in sections 1 – 14 below.

1 INTENTIONALLY LEFT BLANK

2 MAINTENANCE

NFR-2	**Maintenance**	Requirements related to ITSM system outages
NFR-2.1	Maintenance Outages	The ITSM solution may only be made unavailable with the express written consent of SSC's Change Management Office, in accordance with Canada's change management and release management policies and procedures.

3 BACKUP AND RESTORE

NFR-3	**Data Backups**	Requirements related to backing up and restoring ITSM system data
NFR-3.1	Backup Frequency	The ITSM Tool Solution must be backed up at least once daily. Back-up data must remain available for a period of one year.
NFR-3.2.	Backup Restore	Upon request by the Technical Authority, the Contractor must restore the ITSM Solution or data associated with the ITSM Solution to the state of any day in the 365 calendar days preceding the restore request. The Contractor must initiate the restore within 1 hour of the request.
NFR-3.3.	Backup Redundancy	Backups will be stored redundantly according to SSC's backup policies and procedures.

4 DISASTER RECOVERY

NFR-4	**Disaster Recovery**	Requirements related to recovering the ITSM solution from a Disaster situation
NFR-4.1	Disaster Recovery	TBD

5 SUPPORTABILITY

NFR-5	**Supportability**	Requirements related to service supportability, including specific metrics necessary for design and operations.
NFR-5.2	Portability	The ITSM Tool solution must be able to be copied or moved to a completely separate set of infrastructure providing the same functionality and service as the source ITSM instance. -- The ITSM solution must be able to be copied or moved to a different set of infrastructure in a different location in 8 hours or less. This assumes any hardware and components that aren't the responsibility of the contractor are available.
NFR-5.3	Auditability	The following information must be available at all times, including when the solution is unavailable (unless otherwise specified): - All system warnings and errors over the previous 72 hours for all components of the ITSM Tool solution - Currently logged in users (only applies when solution is available) - All login attempts for previous 90 days
NFR-5.4		Intentionally left blank
NFR-5.5	Configurability in live environments	The ITSM solution must be able to be configured in a way that doesn't require service outages, restarts or downtime. This includes adding, updating or removing the following types of configuration, at a minimum: - Incident, Request, Change Request, Problem and CMDB record classification data (Impact/Urgency/Categorization) - Request and Change Request approval workflows and rules - Incident, Request, Change Request and Problem record auto-routing (assignment)rules - Incident, Request and Change Request Service Level Targets - Creating new form fields or hiding existing fields from view - Service Catalogue data (E.g. new or updated information about service offerings which must be reflected on the self-service portal) - Publishing of Knowledge Articles and FAQs - Adding, changing, or removing notifications (including notification content) - Adding or changing reports and their definitions/templates
NFR-5.6	Scalability	The ITSM solution must be capable of providing service to SSC and to other GC partner departments (either as tenants on SSC's ITSM instance or on instances of their own) in a scalable fashion, without impacting/compromising existing installations and their performance. Similarly, the ITSM solution must provide an avenue (technical and logical) for partners to integrate with and/or onboard to SSC's instance of the ITSM tool. Refer to section 3.3 for Volumetric details, including estimated number of Users.

NFR-5	**Supportability**	Requirements related to service supportability, including specific metrics necessary for design and operations.
NFR-5.7	Line of Business Service Management Support	The ITSM solution must provide SSC and GC partner departments with the ability to extend the tool to support line of business service management (e.g. Requests and issues pertaining to Finance, HR, real property)
NFR-5.8	Installation	*TBD*
NFR-5.9	Monitoring	The ITSM solution must allow for the integration with SSC's monitoring tools in such a way that incidents can be automatically created and updated according to defined business rules, and must include the ability to leverage information from CMDB in order to classify and enrich the ITSM records.

6 DATA ARCHIVING

NFR-6	**Data Archiving**	Requirements related to archiving of ITSM records
NFR-6.1	ITSM Archiving Feature	The ITSM Tool must include a configurable feature to allow ITSM records (E.g. Incidents, Service Requests, Tasks) and associated data such as attachments to be archived and retained in a separate repository that is still accessible for reporting purposes. The feature must be configurable on a record type by record type basis. For example there may be different archive requirements for incidents than for problem records.
NFR-6.2	Archiving Policy	TBD

7 PERFORMANCE AND CAPACITY

NFR-7	**Performance & Capacity**	Requirements related to service performance and capacity
NFR-7.1	Capacity and Performance	The response time objective for non-resource intensive functions, such as selecting menus, saving records or navigating to a different view or screen in the ITSM software is 1 second or less.
NFR-7.2	Capacity and Performance	The response time objective for moderate-resource intensive functions, such as browsing the user's personal dashboard or queue, refreshing tables and results lists, searching knowledge base articles in the ITSM software is 3 seconds or less.
NFR-7.3	Capacity and Performance	The response time objective for resource intensive functions, such as generating ad-hoc management reports in the ITSM software is 7 seconds or less.
NFR-7.4	Capacity and Performance	TBD
NFR-7.5	Target Throughput (Production)	The ITSM solution's production environment must initially support the number of users described in 3.2.4 estimated # Users.

8 SYSTEM INTERFACES

NFR-8	**Interfaces**	Other applications the ITSM solution is required to interface with
NFR-8.1	Integration Methods	The ITSM solution 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) • ODBC
NFR-8.2	Multiple LDAP Sources	The ITSM Tool must be able to connect to multiple LDAP sources concurrently.

9 INTENTIONALLY LEFT BLANK

10 SECURITY

NFR-10	**Security**	
NFR-10.1	Security Standards	The ITSM Tool solution must meet the requirements stipulated in the ITSM Security Control Profile, provided as Appendix 5.
NFR-10.2	Email Security	The ITSM Tool's email integration capability must support TLS (Transport Layer Security).

11 USABILITY

NFR-11	**Multi-Platform**	
NFR-11.1	Multi-Platform Support (Web)	The ITSM Solution must be a solution that is fully accessible using a web browser (i.e. all the features and functionalities of the ITSM Solution can be accessed in this way). The Contractor's ITSM Solution must be accessible, at a minimum, by Users who are using 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 solution must make the following functionality available on mobile and tablet devices: - Service request and change request approvals, rejections and comments; - Notification of ticket assignment; - Monitoring of incident, service request and change request queues - Creation and update of incident, service requests and change requests; - View dashboards and reports.

12 USER INTERFACE

NFR-12	**User Interface**	
NFR-12.1.	Localization	The ITSM solution must support both Canadian English and Canadian French, based on individual users' preferences. Localised functionality must include (but is not necessarily limited to): - All ITSM screens accessible by end users - All notification content - Reports - Knowledge Articles and FAQs - Self Service Portal and Service Catalogue
NFR-12.2	Federal Identity Program	The Self-Service Portal must comply 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	GC UI Standards	TBD

13 MULTI-TENANCY

NFR-13	**Multi-Tenancy**	
NFR-13.1	Multi-Tenancy	The ITSM software must include support for multiple, independently configured and used, tenants on the same instance.
NFR-13.2	Access Control	By default, 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. The solution must, through configuration, be able to provide access to specific records that belong to another tenant on the same instance. This access must be able to be given to specific users or groups of users. This configuration must be restricted to an administrator-type permission or role within the solution.

14 TOOL EXTENSABILITY

NFR-14	**Tool Extensibility**	
NFR-14.1	Extensibility	ITSM System Administrators must be able to extend the ITSM product. This includes, but is not limited to: • Ability to build or add screens/forms to the ITSM Tool and apply the ITSM Tool's permission model to them (E.g. – ability to create forms that are accessible to certain types of users, or all users) • Ability to create business rules and/or workflows on forms that have been added to the ITSM Tool by a system administrator post-installation o Business rules and workflows built on forms/screens created by a system administrator must be able to interact or invoke business rules, workflows and/or code that was originally shipped with the ITSM Tool software. • Ability to add fields to forms that were shipped with the ITSM Tool software • Ability to alter the layout of screens that were originally shipped with the ITSM software. This includes, but is not limited to: o Making the screen larger or smaller o Moving fields that were shipped with the software, or hiding them from view o Add or remove columns on tables or lists o Modify the order in which columns appear in tables Modify table sort and/or qualification properties
NFR-14.2	Component Incorporation	ITSM System Administrators must be able to incorporate 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-14.3	Mobile	ITSM System Administrators must be able to incorporate extended components into the ITSM Tool's mobile device user interface, including all associated business rules, workflows and code.

APPENDIX 2 – ITSM TOOL FUNCTIONAL REQUIREMENTS

This Appendix (sections 1 – 13) identifies the functional requirements (e.g. the tasks, functions or actions) that the Enterprise ITSM Tool software must meet in order to support SSC's identified business requirements.

Note: The functional requirements identified in each of the subsections below align with SSC's ITSM Process Evaluation initiative.

1 GENERAL

Functional Requirements: General		
ID	**Name**	**Description**
FR-1.1	Bilingual	The ITSM Tool software must have the capability for 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).
FR-1.2	Search Capabilities	The ITSM Tool software must have the capability to provide 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 o Search across service catalog o Search across knowledge base articles/FAQs/bulletin board/broadcasts - Queues/consoles o Saved searches o Role based searches and views
FR-1.3	Integration with Customer ITSM Tools	The ITSM Tool software must have the capability to support standardized process and ITSM tool interface that enables two-way 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 software must have the capability to provide 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 software must be able to create and update tickets (e.g. incidents, service requests, changes) via email.
FR-1.6	Voice Recognition	The ITSM Tool software 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 software must have the capability to identify user categories that will permit the separation of (e.g. access and permissions) the following four types of users ("user categories): 1. System Administrators – users responsible for system-level solution configuration and coding. 2. Process Administrators – users responsible for: a. ITSM process configuration, and b. Data management (E.g. Employees, Resolver Groups, Locations, etc)

Functional Requirements: General		
ID	**Name**	**Description**
		3. Process Users – users utilizing the ITSM processes such as process and operational staff. Within this category the ITSM software must allow Process Administrators to differentiate between general process users (Resolver group team members) and Team-Lead/Manager users having additional privileges (E.g. assigning tickets to other resolver groups) 4. Process Approvers – users responsible for approving requests, change requests, and 5. End users – representing customer users, the primary users of the self-service portal
FR-1.8	User Notifications	The ITSM Tool software must of the ability to configure, at process level, when users should receive notifications from the system.
FR-1.9	Business Rule Configuration	Able to define business rules such as field validation via a UI accessible by business users (don't need system access)
FR-1.10	Mobile-based Approvals	The ITSM tool must provide 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, in a visual calendar format, 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.

Functional Requirements: General		
ID	**Name**	**Description**
FR-1.14	Queue Management	The ITSM tool must include customizable screens 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 allow 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	Users must be able to visualize impacted end-users/services directly 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.

2 SELF-SERVICE PORTAL (SSP)

Functional Requirements: Self-Service Portal (SSP)		
ID	**Name**	**Description**
FR-2.1	Portal for End Users	The ITSM Tool software 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 software must provide customers/end-users with the ability to order goods and services from various non-IT lines of business (e.g. HR, Facilities).
FR-2.3	Search Capability	The ITSM Tool software must have the capability for 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 software must have the capability to associate 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 software must have the capability to develop, deliver and manage end user satisfaction surveys (e.g. incident closure).
FR-2.6	Capture End User Feedback	The ITSM Tool software must have the capability to provide a "suggestion box" for soliciting feedback on process and interface.
FR-2.7	Chat Support	The ITSM Tool software must have the capability to provide “chat” support for self-service usage.
FR-2.8	Bulletin Board Functionality	The ITSM Tool software must have the capability to publish service related information including outages, scheduled downtimes and other issues.
FR-2.9	External Partner/Public Use	The ITSM Tool software must have the capability 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 software must have the capability 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 software must utilize role-based security to control access to the service catalogue.
FR-3.3	Organizing Services	The ITSM Tool software must have the capability to organize services into logical groupings or hierarchical structures. This must be reflected in the self service portal.
FR-3.4	Service Definition	The ITSM Tool software must have the capability to have configurable service definition templates out of the box.
FR-3.5	Service Entitlements	The ITSM Tool software must allow 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 must be flexible in terms of how they are assigned (e.g. location, Org unit, etc.)
FR-3.6	Structured Content	The ITSM Tool software must have the capability 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 software must have the capability to support different service levels for the same service (e.g., bronze, silver, gold levels).
FR-3.8	Search Capability	The ITSM Tool software must have the capability to quickly find services via a search engine.
FR-3.9	Request Service	The ITSM Tool software must have the capability to create and track service requests through the service catalogue via the self-service portal.
FR-3.10	Multifunction Support	The ITSM Tool software must have the capability for the service catalogue to support multiple business line (example: IT, HR, facilities, procurement).
FR-3.11	CMDB Integration	The ITSM Tool software must have the capability 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 software must have the capability to handle different service states (for example, services in design versus services in production).
FR-3.13	Business Line Support	The ITSM Tool software must have the capability for 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 software must have the capability 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 software must have the capability to create 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 software must have predefined standard reports for users and administrators.
FR-4.4	Export Capability	The ITSM Tool software must have the capability 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 software must have the capability to "drill down" on reports and dashboards from within the ITSM software's UI
FR-4.6	External Data Integration	The ITSM Tool software must have the capability to integrate with external data sources.
FR-4.7	Business Analytics	The ITSM Tool software must have the capability to support business analytics (business intelligence tools).
FR-4.8	Restrict Access	The ITSM Tool software must have the capability to restrict access to reports by role.
FR-4.9	Scheduled Report Subscription	The ITSM Tool software must have the capability for users to subscribe to scheduled reports.
FR-4.10	Report Scheduling	The ITSM Tool software must have the capability to produce scheduled reports which are made available automatically to subscribers.
FR-4.11	Historical Reporting	The ITSM Tool software must have the capability for 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 software must have the capability for real-time reporting via graphical and configurable dashboards.
FR-4.13	Dashboard Display	The ITSM Tool software must have the capability to provide 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 software must have the capability to provide 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 software must store incidents and requests separately, as different record types.
FR-5.2	Incident Records	The ITSM Tool software must have the capability to create, classify, update and close or cancel incident records.
FR-5.3	Incident Record Creation	The ITSM Tool software 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 software must have the capability 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 software must have the capability to link incidents to problems, knowledgebase, known workarounds and change records.
FR-5.6	Link Incidents to Services/CIs	The ITSM Tool software must have the capability 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 software must have the capability 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 software must have the capability to view impacted CIs from within an incident record, and to view upstream and downstream affected CIs and services through a visual depiction.
FR-5.9	Incident Categorization	The ITSM Tool software must have the capability to categorize incidents based on a standard categorization scheme.
FR-5.10	Incident Prioritization	The ITSM Tool software must have the capability 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 software must have the capability 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 software must have the capability 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 software must have the capability 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 software must have the capability 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 software must have the capability to support 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 software must have the capability to input free text, screen captures, and file attachments for the recording of incident descriptions and resolution activities.

Functional Requirements: Incident Management (IM)		
ID	**Name**	**Description**
FR-5.17	Time Tracking	The ITSM Tool software must have the capability 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 software must have the capability to access knowledge and/or support scripts for incident diagnosis and resolution.
FR-5.19	Multiple Sequential Assignments	The ITSM Tool software must have the capability to manage and maintain multiple sequential assignments for each open Incident.
FR-5.20	Collaboration	The ITSM Tool software must provide the ability for members of multiple resolver groups to collaborate on a single incident
FR-5.21	Hierarchical Escalation Notification	The ITSM Tool software must have the capability for hierarchical notification about incidents that exceed or will soon exceed priority/service level parameters.
FR-5.22	Hold Status	The ITSM Tool software must have the capability 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 software must have the capability 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 software must have the capability to trigger a notification to the user when a ticket is placed in a resolved status.
FR-5.25	Automated Ticket Closure	The ITSM Tool software must have the capability 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 software must have the capability to use configurable closure categorization codes upon incident closure.
FR-5.27	Survey Capability	The ITSM Tool software must have the capability to collect end-user satisfaction feedback upon the close of an incident.
FR-5.28	Incident Reactivation	The ITSM Tool software must have the capability to reactivate incident in resolved status.
FR-5.29	Event/Incident Integration	The ITSM Tool software 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 software must have the capability to allow users to submit incidents and view their status via a self-service portal.
FR-5.31	Email Support	The ITSM Tool software must have the capability for users to submit incidents via email and also receive timely updates, through email system integration.
FR-5.32	Change/Problem Creation	The ITSM Tool software must have the capability to create a change or problem from an incident with automatic population of fields.
FR-5.33	Problem Management Integration	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate 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.

Functional Requirements: Incident Management (IM)		
ID	**Name**	**Description**
FR-5.35	Service Asset and Configuration Management	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability 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 software must have the capability 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 software must have the capability to create, classify, approve, update, and close or cancel service request records.
FR-6.2	Service Request Record Creation	The ITSM Tool software 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 software must have the capability to submit attachments as part of a service request and have them stored in the record.
FR-6.4	Request Models	The ITSM Tool software must have the capability 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 software must have workflow capability which allows definition of a service request 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 software must have the capability to limit viewing, creating and editing requests only to authorized requestors.
FR-6.7	Service Request Categorization	The ITSM Tool software must have the capability to categorize service requests based on a standard categorization scheme.
FR-6.8	Service Request Prioritization	The ITSM Tool software must have the capability to prioritize service requests based on a standard prioritization scheme that is derived from the assessment of business impact and business urgency.

Functional Requirements: Request Fulfillment (RFL)		
ID	**Name**	**Description**
FR-6.9	Request Automation	The ITSM Tool software must have the capability to automatically send, receive and log approvals for requests.
FR-6.10	Automation Override	The ITSM Tool software must have the capability to manually override automation, when required.
FR-6.11	Automatic Routing	The ITSM Tool software must have the capability to automatically route requests for appropriate authorization and fulfillment.
FR-6.12	Task Assignment	The ITSM Tool software must have the capability 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 software must have the capability 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 software must have the capability to see countdown time left on fulfillment time (associated with service level targets) and trigger automated escalation if target is breached.
FR-6.15	Automated Status Updates	The ITSM Tool software must have the capability to provide automated status updates to requestors when a request reaches specific points in the workflow.
FR-6.16	Request Cancellation	The ITSM Tool software must have the capability for users to cancel a service request through the self-service portal.
FR-6.17	Service Catalogue and Self-Service Portal Integration	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability to integrate 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 software 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 software must have the capability to create, classify, approve, update and close or cancel change records.
FR-7.2	Change Record Creation	The ITSM Tool software must have the capability for 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 software must have the capability to link change records to impacted service(s), CIs, and group of CIs.
FR7.4	View Impacted CIs	The ITSM Tool software must have the capability 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 software must have the capability to categorize changes based on a standard categorization scheme.
FR-7.6	Change Prioritization	The ITSM Tool software must have the capability 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 software must have the capability to configure the parameters upon which risk is calculated by the tool considering business impact, affected application/business services criticality, collision, historical change information, and compliance with maintenance windows and black-out periods.
FR-7.8	Risk and Impact Analysis	The ITSM Tool software must have the capability 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 software must have the capability to enter of free form text, screen captures, and file attachments for recording of change request descriptions.
FR-7.10	Templated Change Workflow	The ITSM Tool software 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 software must have the capability 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 software must have the capability 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 software must have the capability to store back-out procedures, installation and turnover documents within the change record.
FR-7.14	CAB Support	The ITSM Tool software must have the capability to support a CAB (i.e., approvals/issues submitted and stored electronically).
FR-7.15	Role-based Approval	The ITSM Tool software must have the capability to have multiple role-based approvers and electronic routing of those approvals.
FR-7.16	Automated Approval Workflow	The ITSM Tool software must provide Automated Approval workflow capabilities including:

Functional Requirements: Change Management (CHGM)		
ID	**Name**	**Description**
		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 software must have the capability 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 software must have the capability 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 software must have the capability to provide proactive notification to stakeholders and change advisory board (CAB) members for changes with significant business impact, collisions and compliancy issues.
FR-7.20	Change Calendar	The ITSM Tool software must have the capability to provide 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 software must have the capability to allow for scheduling of recurring events, such as certain types of maintenance.
FR-7.22	Microsoft Exchange Integration	The ITSM Tool software 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 software must have the capability to 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 must support the ability to define and enforce maintenance, release and moratoriums for freeze windows.
FR-7.25	Promote to a Release	The ITSM Tool software must have the capability 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 software must have the capability 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 software 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 software must have the capability to send automated notifications at the scheduled start time to all identified activity assignees to remind them of the change.

Functional Requirements: Change Management (CHGM)		
ID	**Name**	**Description**
FR-7.29	Automated Notifications (Implementation)	The ITSM Tool software must have the capability to send automated notifications upon individual change task completion, and overall change implementation completion.
FR-7.30	Link to Projects	The ITSM Tool software must have the capability to link change records to projects.
FR-7.31	Status Tracking	The ITSM Tool software must have the capability 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 software must have the capability 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 software must have the ability 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 software must have the capability to integrate 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 software must have the capability to integrate with Request Fulfillment allowing for the creation of a change record where required to fulfill a request.
FR-7.36	Problem Management Integration	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability 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 software must have the capability 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 software must have the capability to 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 software must provide a data model capability 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 software must have the capability to display CI fields based on a CI type.
FR-8.4	Create New CIs	The ITSM Tool software must have the capability to create new CIs (including fill in all field values) by designated users.
FR-8.5	Data Validation Rules	The ITSM Tool software must have the capability to enforce data validation rules on field values on creation of any new CI.
FR-8.6	Edit CI Field Values	The ITSM Tool software must have the capability to edit any existing CI field values by varying degrees by authorized users.
FR-8.7	CI Dependencies	The ITSM Tool software must have the capability to define the dependency relationship between CIs in both directions using custom terminology (i.e. hosted on, hosts).
FR-8.8	Graphical View of Dependencies	The ITSM Tool software must have the capability to provide a graphical representation of the dependencies between CIs
FR-8.9	Automated Alerts	The ITSM Tool software must have the capability 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 software must have the capability to assign maintenance windows to any CIs.
FR-8.11	Freeze CIs	The ITSM Tool software must have the capability to "freeze" a CI so that it cannot have a change logged against it.
FR-8.12	Auto Discovery	The ITSM Tool software must have the capability to auto discover CIs in the environment. The ITSM solution must be able 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 solution must possess configuration-based means to ensure that discovered CIs are populated in the CMDB with valid data (classification, product catalog references, etc.).
FR-8.13	Reconciliation	The ITSM solution must be able 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 solution 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 solution must be able to receive CI and relationship data from a variety of sources and configure the reconciliation rules differently for each.

Functional Requirements: Service Asset and Configuration Management (SACM)		
ID	**Name**	**Description**
FR-8.15	Set Workflow Triggers	The ITSM Tool software must have the capability 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 software must have the capability 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 software must have the capability to maintain an audit trail of change requests made to a CI over time.
FR-8.18	Search Capability	The ITSM Tool software must have the capability to search for a CI by any CI field, or combination of fields.
FR-8.19	Ad Hoc Queries	The ITSM Tool software must have the capability to perform ad hoc/general queries.
FR-8.20	Data Import / Export	The ITSM Tool software must have the capability to support both flexible data import/export including: - Flexible file types (XML, csv) - Scheduled/Automated import jobs
FR-8.21	Incident Management Integration	The ITSM Tool software must have the capability to integrate 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.
FR-8.22	Problem Management Integration	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability to integrate with Request Fulfillment allowing for the linking of service requests to CI records.
FR-8.27	Service Catalogue Integration	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate with Knowledge Management allowing for the linking of knowledge to CI records.
FR-8.29	Asset Tracking	The ITSM Tool software must have the capability 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 software must have the capability to support release impact analysis, planning, rollout and deployment activities.

Functional Requirements: Service Asset and Configuration Management (SACM)		
ID	**Name**	**Description**
FR-8.31	Contracts and Licensing Agreements	The ITSM Tool software must have the capability 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 software must have the capability to track the physical location of contracts and agreements, and identify the individuals responsible for them.
FR-8.33	Software Audit	The ITSM Tool software 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 software must have the capability 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 software must have the capability 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 software must have the capability to group 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 software must have the capability to manage leases, depreciation schedules, warranties, and service provider contracts.
FR-8.38	Track Asset/ CI Costs	The ITSM Tool software must have the capability to track both fixed and variable costs of assets/CIs.
FR-8.39	Barcode Scanners	The ITSM Tool software must have the capability to interface with and make use of barcode scanners to scan barcodes from Asset Tags or Serial Numbers.

9 SERVICE LEVEL MANAGEMENT (SLM)

Functional Requirements: Service Level Management (SLM)		
ID	**Name**	**Description**
FR-9.1	Agreements and Contracts	The ITSM Tool software must have the capability to store agreements and contracts.
FR-9.2	Store SLM information in CMDB	The ITSM Tool software must have the capability 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 software must have the capability 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 software must have the capability 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 software must have the capability 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 software must 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 software must have the capability 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 software must have the capability 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 software must have the capability to publish different service levels for the same service.
FR-9.10	Search Engine	The ITSM Tool software must have the capability to incorporate a search engine to facilitate locating service information.
FR-9.11	Multiple Contracts	The ITSM Tool software must have the capability to define multiple contract types and contracts per customer.
FR-9.12	Priority Definitions and Action Times	The ITSM Tool software must have the capability to handle different priority definitions and action times for each customer.
FR-9.13	Agreement and Contract Review	The ITSM Tool software must have the capability to schedule agreement and contract review cycles and renewals.
FR-9.14	Service Level Achievement Against Target	The ITSM Tool software must have the capability 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 software 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 software must have the capability to integrate monitoring tools with service/CI dependency mapping (CMDB) to identify which customer-facing service(s), is impacted by the event.

11 KNOWLEDGE MANAGEMENT (KM)

Functional Requirements: Knowledge Management (KM)		
ID	**Name**	**Description**
FR-11.1	Search Capability	The ITSM Tool software must have the capability 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 software must provide 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 software must have the ability for 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 software must have the capability to create a knowledge article via a fill-in-the-blank template.
FR-11.5	Role-based Knowledge	The ITSM Tool software must have the capability to 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 software must have the capability to create knowledge management entries from incident, problem, request fulfillment and change modules.
FR-11.7	Article Lifecycle Management	The ITSM Tool software must have the capability to manage full life cycle of knowledge articles through administration capabilities (e.g., submission, editing, review, approval, publishing, usage monitoring, etc.).
FR-11.8	Search other Databases	The ITSM Tool software must have the capability for the tool's knowledge management database to search other knowledge bases in the environment.
FR-11.9	Rich-text Editor	The ITSM Tool software 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 software 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.

Functional Requirements: Knowledge Management (KM)		
ID	**Name**	**Description**
FR-11.11	Graphical Workflow	The ITSM Tool software must have the capability 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 software must have the capability to make certain fields in the knowledge article template mandatory.
FR-11.13	Embed Web Links, Images and Objects	The ITSM Tool software must have the capability to embed Web links, images and objects into knowledge articles (e.g., screenshots, etc.).
FR-11.14	Search Capability	The ITSM Tool software must have the capability to search across all sections of a knowledge article from a single search field.
FR-11.15	Feedback Mechanism	The ITSM Tool software must have the capability to allow user feedback to rate/score content for usefulness related to the inquiry.
FR-11.16	Knowledge-Centered Support	The ITSM Tool software must have the capability 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 software must have the capability to create, update, and close or cancel problem records.
FR-12.2	Problem Record Creation	The ITSM Tool software 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 software must have the capability to support 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 software must have the capability 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 software must have the capability 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 software must have the capability to link problems/known error records to a service(s), CIs, and group of CIs.
FR-12.7	Problem Categorization	The ITSM Tool software must have the capability to categorize changes based on a standard categorization scheme.
FR-12.8	Problem Prioritization	The ITSM Tool software must have the capability to prioritize changes based on a standard prioritization scheme that is derived from the assessment of business impact and business urgency.

Functional Requirements: Problem Management (PM)

ID	Name	Description
FR-12.9	Problem / Known Error Differentiation	The ITSM Tool software must have the capability to differentiate between problems and known errors.
FR-12.10	Task Assignment	The ITSM Tool software must have the capability 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 software must have the capability to use configurable cause codes as input to categorizing a problem.
FR-12.12	Closure Codes	The ITSM Tool software must have the capability to use configurable closure categorization codes upon problem closure.
FR-12.13	Self-Service Portal Integration	The ITSM Tool software must have the capability to integrate with the self-service portal, allowing users to view problems and their status.
FR-12.14	Incident Management Integration	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate 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.
FR-12.16	Service Asset and Configuration Management Integration	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate 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 software must have the capability 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 software must have the capability to create, update, and close or cancel release records.
FR-13.2	Related Changes	The ITSM Tool software must have the capability to log a release so that changes can be identified and related to the release.
FR-13.3	Release Record Capture	The ITSM Tool software must have the capability 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 software must have the capability to attach and store documentation with the release record.
FR-13.5	View Impacted CIs	The ITSM Tool software must have the capability to view impacted CIs through the related change records.
FR-13.6	Task Assignment	The ITSM Tool software must have the capability 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 software must have the capability to change status of release and linked changes, release documentation and release approvals.
FR-13.8	Change Status Notification	The ITSM Tool software must have the capability 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 software must have the capability to search all releases by any release data attribute captured by the tool.
FR-13.10	Release Windows	The ITSM Tool software must have the capability to define release windows (show conflicts that impact when releases can be scheduled).
FR-13.11	Master Release Schedule	The ITSM Tool software must have the capability to create and publish a Master Release Schedule.
FR-13.12	Problem Management Integration	The ITSM Tool software must have the capability to integrate with Problem Management allowing for the linking of problem and known error records to release records.
FR-13.13	Change Management Integration	The ITSM Tool software must have the capability to integrate 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 software must have the capability to integrate with the CMDB to support the association of release records to CI records.
FR-13.15	CMDB Support	The ITSM Tool software must have the capability to validate required information from the CMDB for release build and deployment activities.
FR-13.16	Release Readiness	The ITSM Tool software must have the capability to support the establishment and governance of release readiness criteria.
FR-13.17	Authorization Support	The ITSM Tool software must have the capability to authorize and schedule release deployments in conjunction with the Change Management process.
FR-13.18	Post Deployment	The ITSM Tool software must have the capability to trace and track post deployment activities (e.g. early life support).

APPENDIX 3 – RESOURCE ASSESSMENT CRITERIA

To be provided in final RFP

APPENDIX 4 – DEFINITIONS & ACRONYMS

Term or Acronym	Definition
ITSM Tool Solution	Refers to the overall solution to be provided by the Contractor, including but not limited to: provision of an Enterprise ITSM Tool; System Integration (SI) professional services required to implement the new ITSM Tool solution; and Application Management Services (AMS).
Tool	Refers to the Enterprise ITSM Tool licensed software to be provided by the Contractor.
Release	
Contractor	Refers to the Contractor
Work	Refers to all products and services to be delivered by the Contractor under the contract.
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.

Term or Acronym	Definition
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).
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.

Federal Government Working Day (FGWD)	A calendar day, except for Saturday, Sunday and the following 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 SaaS solution.
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 or Acronym	Definition
	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.
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

ITIL Process Terminology	Definition
	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 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,

ITIL Process Terminology	Definition
	standards, guidelines, activities and work instructions if they are needed.
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 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 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.

ITIL Process Terminology	Definition
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 5 – 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
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
ITSM Overlay (Total)	A marking in this column means the vendor must provide some evidence for this security element
ITSM Overlay (Full)	A marking in this column means neither standard addresses the element and the vendor must provide evidence to SSC that the element is addressed
ITSM Overlay (Partial)	A marking in this column means at least one standard partially addresses the element and the vendor must provide evidence to SSC that the element is addressed

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
AC-1	**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**	CC5.2 CC6.1	A.9.2.1 A.9.2.2 A.9.2.3			

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
			A.9.2.5 A.9.2.6			
AC-2 (1)	X	CC5.2				
AC-2 (2)	X	CC5.2				
AC-2 (3)	X	CC5.2				
AC-2 (4)	X	CC5.2				
AC-2 (5)	X	CC5.3				
AC-2 (7)	X	CC5.4				
AC-2 (12)	X	CC6.1				
AC-3	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	X	
AC-4	X	CC5.1	A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3			
AC-5	X	CC5.1	A.6.1.2			
AC-6	X	CC5.4	A.6.1.2			
AC-6 (1)	X	CC5.4				
AC-6 (2)	X	CC5.1				
AC-6 (5)	X	CC5.4				
AC-6 (9)	X	CC6.1				
AC-6 (10)	X	CC5.1				
AC-7	X	CC5.3	A.6.1.2			
AC-8	X	CC2.3	A.6.1.2			
AC-10	X	CC5.3				
AC-11	X	CC5.3	A.11.2.8 A.11.2.9			
AC-11 (1)	X	CC5.3				
AC-12	X	CC5.3				
AC-14	X	CC5.1				
AC-20	X	CC2.3	A.11.2.6 A.13.1.1 A.13.2.1			

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
AC-20 (1)	X	CC5.6				
AC-20 (3)	X			X	X	
AC-21	X	CC5.4				
AC-22	X	CC5.4				
AT-1	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	CC2.3	A.7.2.2.2 A.12.2.1			
AT-2 (2)	X	CC1.3 CC2.5				
AT-3	X	CC2.3	A.7.2.2*	X		X
AT-4	X	CC2.3				
AU-1	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	CC6.1				
AU-2 (3)	X	CC6.1				
AU-3	X	CC6.1	A.12.4.1*	X		X
AU-3 (1)	X	CC6.1				
AU-4	X	CC6.1	A.12.1.3			
AU-4 (1)	X	CC6.1				
AU-5	X	CC6.1				
AU-6	X	CC6.1	A.12.4.1 A.16.1.2 A.16.1.4			
AU-6 (1)	X	CC6.1				
AU-6 (3)	X	CC6.1				
AU-6 (4)	X	CC6.1				
AU-7	X	CC6.1				
AU-7 (1)	X	CC6.1				
AU-8	X	CC6.1	A.12.4.4			
AU-8 (1)	X	CC6.1				

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
AU-9	X	CC6.1	A.12.4.2 A.12.4.3 A.18.1.3			
AU-9 (2)	X	CC6.1				
AU-9 (4)	X			X	X	
AU-11	X	CC6.1	A.12.4.1 A.16.1.7			
AU-12	X	CC6.1	A.12.4.1 A.12.4.3			
AU-12 (1)	X	CC6.1				
CA-1	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	CC4.1	A.14.2.8 A.18.2.2 A.18.2.3			
CA-2 (1)	X	CC4.1	A.18.2.1 E			
CA-2 (2)	X	CC4.1				
CA-2 (3)	X	CC4.1				
CA-3	X	CC7.1	A.13.1.2 A.13.2.1 A.13.2.2			
CA-3 (3)	X	CC7.1				
CA-3 (5)	X	CC5.6				
CA-5	X	CC4.1				
CA-6	X	CC7.4				
CA-7	X	CC4.1				
CA-7 (1)	X	CC4.1				
CA-8	X	CC4.1				
CA-8 (1)	X	CC4.1				
CA-9	X	CC7.1				
CM-1	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	CC7.4				

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
CM-2 (1)	**X**	CC7.2 CC7.3 CC7.4				
CM-2 (2)	**X**	CC7.4				
CM-3	**X**	CC7.4	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4			
CM-3 (2)	**X**			**X**	**X**	
CM-3 (4)	**X**	CC7.1				
CM-3 (6)	**X**	CC7.4				
CM-4	**X**	CC7.1	A.14.2.3			
CM-4 (2)	**X**			**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**	**X**	
CM-5 (5)	**X**	CC7.4				
CM-6	**X**	CC5.1 CC7.4				
CM-6 (1)	**X**	CC7.4				
CM-7	**X**	CC5.1 CC7.1	A.12.5.1*	**X**		**X**
CM-7 (1)	**X**	CC7.3				
CM-7 (2)	**X**	CC5.1				
CM-7 (5)	**X**	CC5.1	A.12.5.1 E			
CM-8	**X**	CC5.1	A.8.1.1 A.8.1.2			
CM-8 (1)	**X**	CC7.4				
CM-8 (3)	**X**	CC6.1 CC6.2				
CM-8 (5)	**X**	CC7.4				
CM-8 (6)	**X**			**X**	**X**	
CM-9	**X**	CC7.4	A.6.1.1*	**X**		**X**
CM-10	**X**	CC3.1	A.18.1.2			
CM-10 (1)	**X**	CC3.1				

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
CM-11	X	CC5.8	A.12.5.1 A.12.6.2			
CM-11 (1)	X			X	X	
CM-11 (2)	X			X	X	
CP-1	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	CC3.1 CC3.3	A.6.1.1 A.17.1.1 A.17.2.1			
CP-2 (1)	X	CC3.1				
CP-2 (2)	X	A1.1	A.12.1.3 E			
CP-2 (3)	X	CC3.1				
CP-2 (4)	X			X	X	
CP-2 (5)	X			X	X	
CP-2 (6)	X			X	X	
CP-2 (8)	X	CC3.1				
CP-3	X	CC1.3	A.7.2.2*	X		X
CP-4	X	A1.3	A.17.1.3			
CP-4 (1)	X	A1.3				
CP-10	X	CC3.1	A.17.1.2			
IA-1	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	CC5.3	A.9.2.1			
IA-2 (1)	X	CC5.3				
IA-2 (2)	X	CC5.3				
IA-2 (3)	X	CC5.3				
IA-2 (8)	X	CC5.3				
IA-2 (9)	X	CC5.3				
IA-2 (11)	X	CC5.3				
IA-3	X	CC5.1				
IA-4	X	CC5.1 CC5.2	A.9.2.1			

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
IA-4 (4)	**X**	CC5.2				
IA-5	**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**	CC5.1 CC5.3				
IA-5 (2)	**X**	CC5.1 CC5.3				
IA-5 (3)	**X**	CC5.2				
IA-5 (6)	**X**	CC5.1				
IA-5 (7)	**X**	CC5.1 CC7.1				
IA-5 (9)	**X**			**X**	**X**	
IA-6	**X**	CC5.3	A.9.4.2			
IA-7	**X**	CC5.1	A.18.1.5			
IA-8	**X**	CC5.3	A.9.2.1			
IA-8 (100)	**X**			**X**	**X**	
IR-1	**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**	CC1.3	A.7.2.2*	**X**		**X**
IR-3	**X**	CC6.2				
IR-3 (2)	**X**	CC6.2				
IR-4	**X**	CC6.2	A.16.1.4 A.16.1.5 A.16.1.6			
IR-4 (4)	**X**	CC6.2				
IR-4 (8)	**X**	CC6.2				
IR-3 (2)	**X**	CC6.2				
IR-5	**X**	CC6.2				
IR-6	**X**	CC6.1	A.6.1.3 A.16.1.2			
IR-6 (2)	**X**	CC6.2				
IR-7	**X**	CC6.1				
IR-8	**X**	CC6.2	A.16.1.1			
IR-9	**X**	CC6.2				
IR-9 (1)	**X**	CC6.2				

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
IR-9 (2)	X	CC1.3				
IR-9 (3)	X	A1.2				
IR-9 (4)	X	CC2.3				
IR-10	X			X	X	
MA-1	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			
MA-2	X	CC5.6 CC7.1	A.11.2.4* A.11.2.5*	X		X
MA-3	X	CC7.1				
MA-3 (1)	X	CC5.6				
MA-3 (2)	X	CC5.8				
MA-3 (3)	X	CC5.6				
MA-4	X	CC5.1 CC5.3 CC6.1				
MA-4 (2)	X	CC7.4				
MA-4 (4)	X			X	X	
MA-4 (6)	X	CC7.4				
MA-5	X	CC1.4 CC5.6				
MA-5 (1)	X	CC7.4				
MA-5 (5)	X			X	X	
MA-6	X	A1.2	A.11.2.4			
PL-1	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-8 (1)	X	CC5.1				
PS-1	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	CC1.4				
PS-3	X	CC1.4	A.7.1.1			

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
PS-4	X	A1.2 CC5.2 CC5.4 CC5.6	A.7.3.1 A.8.1.4			
PS-5	X	CC5.4 CC5.5	A.7.3.1 A.8.1.4			
PS-6	X	CC1.4	A.7.1.2 A.7.2.1 A.13.2.4			
PS-7	X	CC1.2 CC1.4 CC4.1 CC5.5	A.6.1.1* A.7.2.1*	X		X
PS-8	X	CC1.1	A.7.2.3			
RA-1	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			
SA-1	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	CC1.3 CC3.3				
SA-3	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	CC7.1	A.14.1.1 A.14.2.7 A.14.2.9 A.15.1.2			
SA-4 (1)	X	CC7.1				
SA-4 (2)	X	CC7.1				
SA-5	X	CC1.3 CC5.1 CC7.1	A.12.1.1*	X		X
SA-8	X	CC7.1	A.14.2.5			

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
SA-9	**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**	CC7.1				
SA-9 (2)	**X**	CC7.1				
SA-9 (3)	**X**			**X**	**X**	
SA-9 (4)	**X**	CC3.1				
SA-9 (5)	**X**	CC5.5				
SA-10	**X**	CC7.1 CC7.4	A.12.1.2 A.14.2.2 A.14.2.4 A.14.2.7			
SA-10 (1)	**X**	CC7.1				
SA-11	**X**	CC7.1	A.14.2.7 A.14.2.8			
SA-11 (1)	**X**	CC7.1				
SA-11 (2)	**X**	CC7.1				
SA-11 (5)	**X**			**X**	**X**	
SA-11 (7)	**X**			**X**	**X**	
SA-11 (8)	**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**	**X**	
SA-17	**X**		A.14.2.1 A.14.2.5			
SA-17 (2)	**X**			**X**	**X**	
SA-17 (7)	**X**			**X**	**X**	
SA-18	**X**			**X**	**X**	
SA-22	**X**			**X**	**X**	
SA-22 (1)	**X**			**X**	**X**	
SC-1	**X**	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1			

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
			A.18.1.1 A.18.2.2			
SC-2	**X**	CC5.1				
SC-5	**X**	CC5.1				
SC-6	**X**			**X**	**X**	
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**			**X**	**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**	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**	CC5.7	A.18.1.3			
SC-10	**X**	CC5.1 CC5.6	A.13.1.1			
SC-12	**X**	CC5.1	A.10.1.2			
SC-12 (1)	**X**			**X**	**X**	
SC-12 (2)	**X**	CC5.1				
SC-12 (3)	**X**	CC5.1				
SC-13	**X**	CC5.1	A.10.1.1 A.14.1.2 A.14.1.3 A.18.1.5			
SC-17	**X**	CC5.1	A.10.1.2			
SC-18	**X**	CC5.8				
SC-19	**X**	CC5.1				
SC-20	**X**	CC5.1 CC5.6				

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
SC-21	X	CC5.1				
SC-22	X	A1.1				
SC-23	X	CC5.1 CC5.3				
SC-23 (1)	X	CC5.3				
SC-23 (3)	X	CC5.3				
SC-28	X	CC5.1	A.8.2.3*	X		X
SC-39	X	CC5.1				
SI-1	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	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			X	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			X	X	
SI-4 (9)	X			X	X	
SI-4 (11)	X			X	X	
SI-4 (12)	X	CC6.1				
SI-4 (13)	X			X	X	
SI-4 (16)	X	CC6.1				
SI-5	X	CC6.1 CC7.3	A.6.1.4*	X		X
SI-6	X	CC6.1 CC6.2				
SI-7	X	CC6.1				

Security Control ID	Vendor Responsible to Address for the Application Layer	AICPA SSAE 16 SOC2	ISO / IEC 27001	ITSM Overlay (Total)	ITSM Overlay (Full)	ITSM Overlay (Partial)
SI-7 (1)	**X**	CC6.1				
SI-7 (7)	**X**	CC6.1				
SI-7 (14)	**X**			**X**	**X**	
SI-8	**X**	CC5.8				
SI-8 (1)	**X**	CC5.8				
SI-8 (2)	**X**	CC5.8				
SI-10	**X**	PI1.2				
SI-11	**X**	PI1.1				
SI-12	**X**	PI1.4				
SI-16	**X**	CC5.1				

APPENDIX 6 - EDC SERVICES TECHNICAL INTEGRATION INFORMATION

To follow VIA RFI Amendment

APPENDIX 7 - LEGACY ITSM TOOLS USED AT SSC AND CUSTOMER DEPARTMENTS

ITSM Topic - SSC and Partners Only (SSC Clients/GC Agencies exluded)	**ITSM Metrics**
Estimated total number SSC Infrastructure Configuration Items (CI)	82,000
Estimated total number of annual SSC Service Request and Incident tickets:	500,000

ITSM Tool Used - SSC and Partners Only (SSC Clients/GC Agencies excluded) **Some partners have multiple ITSM tools in place	**# of Partners**
Axios Assyst	9
BMC Remedy	8
BMC Remedy (custom)	2
BMC Service Desk	2
BMC Service Desk Express	1
BMC Track-IT!	1
Frontrange Heat	3
HP Service Manager	4
JIRA	2
LANDESK	2
ManageEngine ServiceDesk Plus	1
ChangeGear	1
Dell Helpdesk Authority	1
Easy Vista	1
HP Open View Asset Centre	1
IBM SmartCloud	1
InfoWeb	2
Microsoft System Center Service Manager	1
OTRS	1
Rochade	1
SAP (Asset Management)	1
SRIMS	1

APPENDIX 8 – ITSM PROCESS USE CASE EXAMPLES

To follow VIA RFI Amendment

APPENDIX 9 - SSC INFRASTRUCTURE SERVICES OVERVIEW

• Service Standards Definitions

Service standards are as follows.

• Availability

Percentage of time, during service hours that the service performs its agreed function. Percentage is calculated using the agreed service time, which excludes planned downtime (e.g. maintenance) minus actual downtime. Actual downtime considers all service dependencies and the result is based on the lowest common denominator that contributed to service unavailability.

• Service hours

Time period when the service should be available.

• Regular scheduled maintenance

Time period (duration) and frequency when the service should be considered not available due to regular scheduled maintenance. This is an exclusion from service hours.

• External vendor support hours

Time period when support, provided directly to partners by an external vendor, should be available for the service.

• Mean time to restore

The average time taken to restore an IT service or other configuration item after a failure. MTRS is measured from when the configuration item fails until it is fully restored and delivering its normal functionality.

• Request fulfillment duration

Time period after receipt of a request containing correct and complete information that the request should be fulfilled.

Midrange

The Midrange Service is a combination of hosting technologies that form a fully managed platform on which to install an application. The midrange platform can include:

- physical or virtual servers
- secure platform management
- multi-tier platforms
- converged infrastructure
- managed operating systems
- third-party appliances
- disaster recovery

SSC offers multiple choices for platforms. The leading criteria for choosing a platform include:

- Meets the customer’s business requirements
- Contains or minimizes costs by
  - offering a platform meeting planned business requirements
  - offering an “ecosystem” meeting business continuity high availability and disaster recovery (HA/DR) requirements
  - reviewing existing and available capacity to accept new workloads
  - optimization and capacity planning to drive efficiencies and/or optimizing processes
- For new requirements or builds, makes use of standard SSC offerings

Features

The following are available on a cost-recovery basis.

- Infrastructure management
  - Infrastructure support
  - Hardware and operating system maintenance
  - Monitoring of key performance indicators (KPIs)
  - License management up to and including the managed operating system as outlined in the SSC Operating System Roadmap current versions:
    - Windows
    - Linux
    - Unix
- Compute and storage capacity matched to business requirements
- Operational recovery (backups, restores)

- Temporary sandbox environments isolated from application development and test environments, for product evaluations and proof of concept elaborations

Security of information

Midrange services can be utilized for information classified up to and including level of Secret, using the appropriate level of additional security controls.

Service standards

Availability: 24 x 7 x 365, 99.5% of the time

- **Service hours:** 24 x 7 x 365, services are fully operational and continuously monitored
    - hours are negotiated per environment through an official Service Level Agreement
- **Regular scheduled maintenance:** mandatory monthly scheduled maintenance window (minimum 4 hours per data centre) as per agreed Service Agreement

Mean time to restore service:

- varies as defined in Service Level Agreements (SLAs) depending on complexity of the environment

Request Fulfillment Duration:

- variable based on the level of complexity, quantity, resources and other factors applicable to each individual request

Support

Hours of support:

- 12 x 5 response to low- and medium-priority incidents and change requests
- 24 x 7 response to critical and high-priority incidents available on request with signed agreement and funding

Terms and conditions

- The preferred standard consists of virtualized hardware and RedHat Enterprise Linux operating systems.

- SUSE Linux servers are available on requests.
- Physical servers may be deployed as deemed necessary based on specific project/workload requirements.
- Partners are obligated to consult the **SSC OS Roadmap** before deployment efforts to ensure compatibility with the latest operating system standards.
- SSC reserves the right to select the hardware layer.

SSC OS Roadmap

The SSC vision is to provide standardization of OS versions across SSC and its partners and to create a secure, cost-effective, agile, scalable, and innovative service to meet the needs of clients. As per the functional directives, a maximum number of three Operating Systems versions will be supported, namely “N-1”, “N” and “N+1”. “N” is defined as the version that SSC currently deploys for which all the security, data protection and security tools have been developed and released for production purposes by SSC Service Lines.

Currently, SSC is supporting a mixture of hardware and software platforms from various vendors:

Technical Service	**Description**
Windows	Windows pre-2003, 2003, 2008, 2008R2, 2012, 2012R2
Linux	Red Hat Enterprise Linux (RHEL) versions 4, 5, 6, 7
	CentOS (Free RHEL) v 6, 7
	SUSE (SLES) v 10, 11, 12
	Ubuntu v 12.04,14.04
	Others
UNIX	IBM AIX (on Power) versions 6, 7.1, 7.2
	Solaris (on SPARC) v 10, 11
	HP-UX (on Itanium) v11.31

OS Availability for Development and Production

This version of the OS should be used for development purposes if target application production date is no sooner than the OS target production availability. Production implementation dates for N+1 versions will be between six months to one year from the product release date in order to allow SSC to conduct proper testing and upgrade the required OS management and security tools.

Operating Systems Roadmap

	n-1	n	n+1	n+1	n	n-1
Windows	8	12	17	30/06/2022	01/01/2020	01/01/2018
RHEL	5	6	7	30/06/2022	31/12/2019	31/03/2017
SLES	10	11	12	30/06/2022	31/03/2019	31/07/2016
AIX	6	7.1	7.2	30/06/2022	31/12/2019	30/04/2017
CentOS	5	6	7		31/12/2019	31/03/2017
Ubuntu LTS	12	14	16		01/04/2019	01/04/2017
Debian LTS	6	7	8		30/04/2018	29/02/2016
Solaris	10	11	12		30/06/2019	30/06/2017
HPUX	11.2	11.3	11.3		30/06/2019	30/06/2017

• Storage

Storage is an end to end managed infrastructure solution that offers secure, reliable and scalable storage capacity. Storage is offered as a bundle with other SSC services and is not available as a stand-alone service to SSC partners.

While a standard service to all Partners is the desired state, at this time service and service levels may vary between different Legacy data centres and with the Enterprise Data centres. Legacy standards are based on the date of creation by the SSC Order in Council.

Storage is a technical service available internally to SSC. Storage infrastructure provides storage capacity at block level (storage area network) and at file level (network attached storage). Capacity and performance are appropriately sized according to the business requirements provided by SSC partners.

Data protection is included in all storage services.

- ## Features

- Three distinct tiers of capacity performance to align with SSC Partner and client business requirements
- Data protection includes a copy of protected images off-site
- Data protection for data centre storage services has a minimum retention period of 30 days
- No single point of failure within data centre storage infrastructure
- Supports of connection protocols
- Elastic infrastructure and resource pooling to facilitate bursting and scaling
- Management of service, including infrastructure fault monitoring, and analytics for performance and capacity trending
- Infrastructure lifecycle management
- Secure separation of capacity within enterprise datacenter based on security zones and development lifecycle

Optional - Extended retention period of protected images

- ## Security of information

Storage service can be utilized for information classified up to and including level of Protected B-Med/Med using the appropriate level of additional security controls

- ## Service standards

Availability: 24 x 7 x 365, 99.5% of the time

- **Service hours:**
  - **Enterprise data centres**: 24 x 7 x 365, services are fully operational and continuously monitored
- **Regular Scheduled Maintenance:** In general, scheduled maintenance is performed non-disruptively. Individual storage units may be brought out of service in planned outages to perform extraordinary maintenance. The outage frequency is typically approximately once a year and for less than four hours.

Mean time to restore service:

- **Enterprise base service:**
  - Recovery time objective (RTO) - standard: 4 hours
  - Recovery point objective (RPO) - standard: 24 hours

Request Fulfillment Duration:

- Variable based on the level of complexity, quantity, resources and other factors applicable to each individual request. Fulfillment duration may be established during the creation of the business intake request.

Support

SSC Partner data owners should contact ESD to receive support on storage services.

Hours of support:

Enterprise Data Centre

- 12 x 5 response to low- and medium-priority incidents and change requests
- 24 x 7 response to critical and high-priority incidents and recording of low- and medium-priority incidents and change requests

Terms and conditions

- Migration of workloads to end-state data centres is the preferred option to manage growth and obsolescence; however, growth in legacy environments may be supported if customer funding is available and the request aligns with Program Integrity guidelines.
- If approved, procurement of additional capacity for legacy storage is based on historical growth rates in conjunction with the life expectancy of the infrastructure.
- The use of shared virtual storage is mandatory. Dedicated storage for individual workloads and projects should not be procured or deployed.
- Every effort must be made to ensure best practices are applied in the administration of the legacy storage environment, while minimizing expenditures and acquisitions

Data Centre Facility

Data Centre Facility SSC technical service is available internally only. Standard partner usage is addressed through partner-facing services.

Features

- High-density Tier 3 data centre capacity
- Multi-tenant (multiple partners) environment with no physical separation
- Conditioned, uninterrupted power for IT infrastructure
- Full UPS power, back-up systems and N+1 (or greater) redundancy

- Robust heating, ventilation and air conditioning (HVAC) systems
- Security equipment, techniques and procedures to control, monitor and record access to the facility
- Measuring and monitoring of availability, efficiency, capacity and security
- Operations centres and storage space
- A minimum of two separate network carrier access points for redundancy
- A minimum of two data centres configured as a pair, enabling application high availability and disaster recovery

Not included: There is no physical access to the data centres. All access to the systems in support of business programs must be done remotely

Security of information

This service can be used to process information up to Protected A. Information classified at Protected B can be processed using the appropriate level of additional security controls.

Service Evolution

The features of the Data Centre Facility Service will evolve over time. Please consult the data centre services roadmap.

IT Hardware Installation - Planning and installation

This begins once there is an approved solution design and technical details are known (bill of material, data cabling plan, etc.). The complexity of the project will determine how long this takes.

These meetings must be requested and managed by the Customer. SSC Facilities needs 1 week notice to initiate these meetings and an approved project.

Service standards

Availability: 24 x 7 x 365, 100% of the time

- **Service hours:**

Type of data centre	Service hours	Provisioned
Enterprise	24 x 7 x 365	on-site

- **Regular scheduled maintenance:**
  Enterprise: The enterprise data centres are designed such that there are no planned maintenance activities that require a complete outage of the Enterprise Data Centres

(Barrie, Borden and Gatineau).

- **External vendor support hours:**

Type of data centre	Service hours	Provisioned
Enterprise	24 x 7 x 365	on-site

Mean time to restore service:

Type of data centre	Mean time to restore1	Percent of the time
Enterprise	The enterprise data centre facilities are built to be very resilient electrically and mechanically and scenarios that would cause a complete data centre facility failures are extremely limited with a low probability of occurring.	100%

1: If the failure is catastrophic (disaster event), then the repair is measured in months and disaster recovery plans are invoked.

Request fulfillment duration:

Service request	Time to fulfill	Percent of the time
Project initiation / procurement SOW development	• according to SSC Enterprise Business Intake published process times	80%
IT hardware installation - planning	• SSC Facilities needs 1 week notice to initiate meetings for approved projects	80%
Capacity planning	• 15 days	80%
Escort	• Incident response is 1 hour • Planned visit is up to 5 days	90%
Remote hands	• Incident response is 1 hour • Planned visit is up to 5 days	90%
Install IT devices	• 5 to 10 days	90%
Device cabling	• 5 to 10 days	90%
Backbone cabling	• Up to 60 days	80%
Shipping/ receiving	• Minimum 2 business day notice and must be scheduled during posted loading dock hours	90%
Decommission equipment	• Handled as least priority activity, maximum 30 days from request	90%

- Support
- Post initial install - ongoing support

SSC Facilities provides 24 x 7 x 365 facility support that is dispatched through SSC Enterprise Service Desk for items marked "Yes" in the After Hours column in the table below. The customer must follow the lead customer requirement and time requirements when requesting services listed in the table below: Ongoing Support Services

Activity	**Customer Requirements**	**Description**	**After Hrs?**	**Typical Lead Time**
Capacity Planning	• Performed quarterly • 18 month projections required • Subject to Approval and Change Management	Request to engage the Enterprise Data Center Facilities team to gather requirements for future initiatives and operational plans	No	5 days
Escort	• As & when required using SSC access procedures (to be provided post contract award) • Site access requests should be bundled whenever possible to minimize number of site visits.	Following SSC Data Centre site escort procedures provide access to the data center	Yes	• Incident response is 1 hour • Planned visit is up to 5 days
Remote Hands	• As & when required using SSC procedures (to be provided post contract) • Requires a Service Request initated by SSC	Diagnose, configure, troubleshoot, and repair data center equipment	Yes	• Incident response is 1 hour • Planned visit is up to 5 days
Racking & Stack	• Requires an approved SSC change request. • Requests subject to capacity planning approval	Plan equipment layout, add power circuits, unpack, mount, cable, label, and document	No	5-10 days
Device Cabling	• Requires an approved SSC change request.	Intra & inter cabinet cabling, copper and fibre, testing and certification, fully documented cable runs and diagrams	No	5-10 days

Activity	Customer Requirements	Description	After Hrs?	Typical Lead Time
Backbone Cabling	• Requires an approved SSC change request. • Procured and installed by SSC on a cost recovery basis	Expansion of the horizontal cabling infrastructure to accommodate capacity and footprint growth, fully documented and diagramed.	No	Up to 60 days
Shipping/ Receiving	• Provide a **minimum of 2 business days** notice for all shipments.	Secure handling of shipments received at the facility. All shipments must be related to either a) IT Hardware/Component replacement, or b) IT Equipment for an approved implementation ready for immediate integration.	No	Minimum 2 business days notice and must be scheduled during working hours
Decommission Equipment	• Requires an approved SSC change request. • SSC follows Racking & Stacking procedures for delivery of this service. • Media disposal: to be turned over to SSC for disposal. • Decomissioned hardware must be removed from the facility within 48 business hours of completion of the service request.	Remove hardware from service and device media must be handled according to Government of Canada standards.	No	Handled as least priority activity, maximum 30 days from request.

Activity	Customer Requirements	Description	After Hrs?	Typical Lead Time
Hardware Maintenance	• Customer/Hardware Vendor responsibility • Escort required and to be scheduled • Customer/Hardware Vendor must bring necessary hardware and/or components to site as required as no storage space will be provided. • Break/Fix of removable media is subject to defective media retention by SSC	Adding hot swap hardware components, memory expansion, disk expansion, other hardware component expansion, blade components, etc.	Yes	• Incident response is 1 hour • Planned visit is up to 5 days

GC LAN

GC LAN is an enabling service that provides foundational interconnectivity for services such as Wi-Fi, data, voice and video that are transported over the IT infrastructure and are quite critical to day-to-day operations of the Government of Canada.

Features

The standard service components are as follows:

- Wired user network connectivity; for unclassified, Protected A and Protected B traffic
- Centralized Enterprise Management System
- All associated LAN network equipment including provisioning and installation
- Site survey and network design services
- Co-ordination/project management for implementation, acceptance testing, migration plan, etc.)
- Help desk, equipment maintenance and Repair function
- Service ordering process
- Life-cycle management

- Labor and material for the installation, labelling, testing and documenting of new GC-LAN fit-ups.
- Scheduling work, including:
  - Moves, adds and changes (MACs)
  - Re-fit and fit-up projects
  - Break-Fix/Repair
  - Collaboration with clients/partners and/or SSC, building owners and/or managers, cabling technicians, other trades

Service standards

Availability: Baseline availability is 95% unless otherwise specified by individual circumstance and agreed upon with partner and client organizations.

- **Service hours:** 24 x 7 x 365
- **Regular scheduled maintenance:** All regular scheduled maintenance is specific to service, site, and partner.

Mean time to restore service:

- **Repair work**:

Work	**Repair work categories (RWC)**					
	Primary service areas			**Remote service areas (defined as outside major city centres can be impacted by travel time and third-party availability)**		
	Regular	**Priority**	**Emergency**	**Regular**	**Priority**	**Emergency**
MTTA (mean time of arrival during core work hours)	1 work day, 95% of the time is the default, special circumstances could command a higher rate	4 work hours, 95% of the time	2 work hours, 95% of the time	7 work days, 95% of the time	5 work days. 95% of the time	4 work days, 95% of the time
MTTR (mean time to resolution	3 work days, 95% of the time	2 work days, 95% of the time	4 work hours, 95% of the time	9 work days, 95% of the time	7 work days, 95% of the time	4.5 work days, 95% of the time

during core work hours)						

Request fulfilment duration:

- **Project work**: nature and the scope of each project dictates the fulfilment duration
- **MAC work**:

Work	**MAC work categories (MWC)**					
	Primary service areas			**Remote service areas (defined as outside major city centres can be impacted by travel time and third-party availability)**		
	Regular	**Priority**	**Emergency**	**Regular**	**Priority**	**Emergency**
Adds, Changes (up to 20 ports, etc...)	5 work days, 95% of the time is the default, special circumstances could command a higher rate	3 work days, 95% of the time	1work day, 95% of the time	8 work days, 95% of the time	5 work days, 95% of the time	2 work days, 95% of the time

Support

SSC support

- MAC and project work can be consumed during business hours 07:00 to 17:00 (local), Monday to Friday.
- Only break-fix/Repair work can be consumed after business hours.

Cabling

Cabling services provide the foundational transport mechanisms by which voice, data and video signals are transported over the IT infrastructure and are quite critical to day-to-day operations of the Government of Canada.

Features

Material and installation

- Labor and material for the installation, termination, labelling, testing and documenting of new fibre and copper cable runs (horizontal and backbone)
- Moving and removing existing cable runs
- Installation of enclosures, conduit, trays, and other cabling support infrastructure, when necessary
- Cabling work performed by certified network cabling technicians and fibre optic technicians, in accordance with industry standards

Administration and coordination

- Scheduling work, including:
- Moves, adds and changes (MACs)
- Re-fit and fit-up projects
- Repair
- Collaboration with clients/partners and/or SSC, building owners and/or managers, cabling technicians, other trades

Cable plant design

- Standards-based design specifications for fit-up and re-fit of spaces and pathways
- Standards-based design specifications for copper and fibre cabling distribution
- Site surveys for the purpose of:
- Recommending upgrades and/or improvements to the cabling, spaces and pathways
- Preparing design specifications
- Performing large-scale evaluations of existing cable plant facilities

Not included

- Top SECRET networks **Note:** Connectivity between sites is in scope
- Stand-alone closed circuit TV
- Cable TV Services
- Building access control systems (except in data centres)
- All Antenna Systems
- Distance worker data connectivity
- Trenching

Available on a cost-recovery basis

- All cabling project work

Service evolution

As part of the ongoing life-cycle management of the services and contracts, SSC has introduced a new underpinning cabling contract (GCS), to support partners' cabling initiatives.

• Service standards

Availability: 24 x 7 x 365, 100% of the time; based on the physical presence of the cable and not the service hours for support

- **Service hours:** Cabling MAC, repair and project work can be consumed during business hours 07:00 to 17:00 (EST), Monday to Friday. Only repair work can be consumed after business hours.
- **Regular scheduled maintenance:** no regular scheduled maintenance window

Mean time to restore service: based on a regular repair request for a primary service area. For cabling repairs, the MTTRS greatly depends on the status of the site and its surrounding infrastructure as well as by any complications encountered based on this status. Generally, GCS is able to meet expected repair timelines. For all other repair request metrics See: Cabling – Service standard metrics

- 3 business days, 90% of the time

Request fulfilment duration: based on adding one to five cables/drops at a primary service area. For all other request types see: Cabling – Service standard metrics

- 5 business days

RFD is based on adding one to five cables/drops at a primary service area. Please be advised that the Start Date for cabling activities will be dependent on finalized financial information and the availability of materials. For all other request types see: Cabling – Service standard metrics

• Support

SSC support

- Cabling MAC, Repair and Project work can be consumed during business hours 07:00 to 17:00 EST, Monday to Friday.
- Only Repair work can be consumed after business hours.

After-hours repair work

- Partners must communicate first with the Service Manager for after-hours cabling Repair support

Data Centre Network

Data Centre Network (DCN) service provides local area network infrastructure within a data centre environment (Legacy and Enterprise), which enables data communication among local resources within a data centre. The service includes equipment, maintenance, configuration, administration, monitoring, and 24 x 7 support.

The DCN service applies specifically to the following criteria:

- A core with aggregation switching network (L2/3; higher with load balancing)
- Data centres that are greater than 1000 square feet having both UPS and HVAC
- Contains enterprise servers and storage devices running production services (*i.e.* not designated as a lab environment)

Features

Components

- Data Centre Network Connectivity (incl. Core routing, Aggregation switching, Load-balancing) for unclassified, Protected A, and Protected B traffic

- Centralized Enterprise Management System
- All associated Data Centre Network equipment including provisioning and installation
- Site survey and network design services
- Co-ordination/project management for implementation, acceptance testing, migration plan, etc.)

- Help desk, equipment maintenance and Repair function
- Service ordering process
- Life-cycle management

Service management

- 24 x 7 monitoring and management via Network Operations Centre and the Service Desk
- Help desk, equipment maintenance and repair function

- Performance monitoring services
- Post-implementation training
- Change management processes

Provisioning

- Service provisioning, upon successful completion of assessment and design activities. Additional structured cabling and equipment requirements may delay service delivery
- Service quotation and service order process
- Operational coordination and project management
- Equipment provisioning and installation
- Acceptance testing

Optional

The following services are over and above the standard offering and will be paid by partners.

- Post implementation training
- Network encryption above Protected B

Out of scope

- Top SECRET networks
- Stand-alone closed circuit TV
- Cable TV services
- All antenna systems
- Distance worker data connectivity

Service evolution

As part of the ongoing life-cycle management of the services and contracts, SSC will introduce underpinning contracts to support DCN transformation.

- ## Service standards

Availability:

- **Enterprise data centre network**: 24 x 7 x 365, 99.9% of the time
- **Service hours:** Data Center Network standard operation/maintenance and project work can be consumed during business hours 07:00 to 19:00 local time, Monday to Friday. Although SSC's DCN provides on-call support and monitoring 24 x 7 x 365, this level of support is applicable only

to the SSC enterprise data center and critical/high availability services covered under a signed agreement with partner(s).

- **Regular scheduled maintenance:**
    - **Enterprise data center network:** no standard regular scheduled maintenance window

Mean time to restore service (MTRS): is based on the established SSC ITSM model; incidents are categorized as follows and escalated based on service(s) impacted/affected by the incident

- **Low**: 4 business days, 95% of the time
- **Medium**: 2 business days, 95% of the time
- **High**: 8 hours, 95% of the time
- **Critical/major**: 4 hours, 95% of the time

Note MTRS can also vary based on support level agreement signed with partners for critical/high availability services.

Request fulfilment duration: based on the level of effort required by DCN as well as the complexity of the request

- **standard, non-impacting move/add/change**: 5 business days.
- **project work**: the nature and the scope of each project dictates the fulfilment duration

Support

Partner responsibilities:

- Designate a 24 x 7 point of contact for coordinating planned or emergency maintenance
- Provide 24 hour access to facilities
- Submit a request to the SSC Enterprise Service Desk for Moves, Adds and Changes, which may require additional cost

GC WAN

The **GC WAN (Wide Area Network)** service provides enterprise WAN connectivity for data centres and GC buildings and locations. It interconnects users and computers from national and international locations to each other and the Internet, while supporting business applications for simultaneous voice, data and video communications, as required.

Partners and clients are entitled to all features and options. Partners can order upgrades on a cost-recovery basis.

- Features

General

- Standardized service levels and service management processes
- Support for a wide variety of programs and applications, including legacy devices
- Security monitoring and enhanced security controls
- Transmission of data at the Protected A level
- Logical separation of partner/client data
- High speed point to point connectivity for data centers
- Back up and disaster recovery service for data centers

Available on a fee for service or when provided by partner departments

- Upgrades to a higher increment of WAN bandwidths
- Higher availability and diverse connections
- Network encryption, beyond the Protected A baseline

Not included

- Connectivity within buildings or campuses beyond the WAN connection (demarcation point)

Security of information

This service can transmit data up to Protected A. Information classified at Protected B or higher can be transmitted using the appropriate level of additional encryption.

Where GC WAN cannot deliver the contracted commercial WAN services, where they are not cost-effective, or are otherwise not appropriate, connectivity will be provided through the Government of Canada Internet Service (GC IS) or SSC Satellite services.

Service evolution

As part of the Transformation Program, SSC is consolidating the service onto a smaller number of contracts to standardize service management, improve security and generate savings. The first step is to move to a single physical infrastructure, with many logical networks. The next step is to assess the potential to reduce the number of logical networks, and then proceed.

The current GC WAN service is composed of three sub-services, National WAN, International WAN, and Backbone. A fourth sub-service, the GC Science Network (GCSN) will be added in the near to mid-term.

Service standards

Service standard definitions

Availability: 24 x 7 x 365 Availability is site-specific. Objectives range from 99.3%, up to 99.999% for most national locations. Objectives for international locations or locations with satellite service range from 99.8% to 99.999%.

- **Service hours:** 24 x 7 x 365
- **Regular scheduled maintenance:** All regular scheduled maintenance is sub-service-, site- and partner-specific.
- **External vendor support hours:** There is no direct interaction between vendors and partners. SSC receives 24 x 7 x 365 support from vendors.

Mean time to restore service:

- Targets vary depending on site and-or partner profile and geographical area, and range from 1 hour to 48 hours. International locations, satellite locations and very remote national locations (i.e. fly-in locations and unmanned locations, etc.) may experience a substantially greater MTRS.

Request fulfilment duration:

- Varies depending on the location and requested service. International locations may experience a substantially greater duration.
- Service Delivery Intervals (SDIs) can vary based on the type of request, such as a software change, bandwidth upgrade, new service where facilities exists, new service where no facilities exists (build required). The targets range from 5 federal government working days (FGWD) to 80 FWGDs from when the order is submitted to the vendor.

Support

SSC receives 24 X 7 support from the vendors on behalf of the GC. There is no direct interaction between the vendors and Partners or clients.

Connectivity issues identified by Partners and clients should be reported to their organization's service desk.

Service Standards Summary

Service	Availability	Mean Time To Restore Service	Request Fulfillment Duration
Midrange	24x7x365, 99.5%	Variable	Variable
Storage	24 x 7 x 365, 99.5%	**Enterprise:** RTO - 4 hours RPO - 24 hours **Legacy:** Variable	Variable
Data Centre facility	24 x 7 x 365, 100%	**Enterprise:** No time given. Not likely to occur - 100% **Legacy:** 8-12 hours (where support contracts in place) - 70% 12-24 hours (best effort, no support contract in place) - 50%	Variable
GC LAN	24x7x365, 95%	Variable	Variable
Cabling	24 x 7 x 365, 100%	3 business days, 95% of the time	5 business days

Service	Availability	Mean Time To Restore Service	Request Fulfillment Duration
Data Centre Network	**Enterprise data centre network**: 24 x 7 x 365, 99.9% of the time **Legacy data centre network**: 24 x 7 x 365, 95% of the time	**Low**: 4 business days, 95% of the time **Medium**: 2 business days, 95% of the time **High**: 8 hours, 95% of the time **Critical/major**: 4 hours, 95% of the time	5 business days
GC WAN	24 x 7 x 365 Availability is site-specific. Objectives range from 99.3%, up to 99.999% for most national locations	Targets vary depending on site and-or partner profile and geographical area, and range from 1 hour to 48 hours.	Various

- ## References

For further information please consult: http://service.ssc-spc.gc.ca/en/services