[STREAM A] ANNEX A – STATEMENT OF WORK

Shared Services Canada (SSC)

Summary of Service Desk Requirements

1.0 General Requirements

- **Baseline Volumes:** the Contractor must have the capacity to handle current contact volumes, and will be required to accommodate growth in volumes.
- **Resourcing Elasticity:** the Contractor must have the capacity to accommodate increases in contact volumes (up to 30%) for short or long term events (i.e. Olympic Games, G-7, G-20, Elections, Francophone Games etc.) with 90 days notification of increased capacity requirements and duration thereof.
- **Support emergency/crisis situations**: The Government of Canada mobilized resources quickly to address the COVID-19 crisis. The Contractor must have the capability to support these types of situations and allocate resources when necessary. During these times, a Heightened Awareness Window (HAW) is enforced to ensure that technical teams respond quickly in the event of an incident (no matter the priority) affecting a particular Service, Application, etc. Although the HAW will trigger an immediate response, it is still integrated with the existing Incident Management process. The Contractor will make available manager/supervisor/agents level resources for reporting and status of the service desk as well as to relay operational changes needed to be implemented by the service desk.
- **Hours of Operation (ESD):** the Contractor must provide ESD support services 24 Hours a day, 7 days a week, and 365 days a year (including all holidays) to Partner Service Desk Agents.
- **Hours of Operation (EUSD):** the Contractor must provide EUSD support services to end-users during established Core Business Hours for EUSD Customers (excluding weekends and Federal Statutory Holidays).
- **Language:** the Contractor must provide support services to users of the ESD and EUSD in the official language of their choice. Those support services, including all written and verbal communications, must be of equal quality and level of service in English and French, at all times.
- **Service Level Requirements:** Contractor service/performance shall be managed through a Service Level Agreement establishing Minimum Service Levels on multiple Service Level Categories relating to response times, resolution rates, quality and customer satisfaction.
- **Remediation:** the Contractor shall be responsible for ensuring that performance meets or exceeds Minimum Service Levels in each month of the Contract Term. The Contractor is responsible for the cost and expense for all actions relating to the reporting and remediation of Service Level Failures.
- **Chronic Service Level Failure:** in the event of Chronic Service Level Failures (2 or more consecutive months), the Contractor must deploy specialized management and non-operational resources to address chronic Service Level Failures. The Contractor will be responsible for the cost and expense of deploying these additional resources. For persistent service quality issues and failure to remediate/resolve root causes resulting in Chronic Service Level Failures, SSC may invoke the Termination for cause clause of the Agreement.
- **Quality Assurance:** the Contractor shall implement prescribed Quality Assurance processes and procedures and shall participate in the enhancement of those processes and procedures over the duration of the Contract Term.
- **Metrics Repository**: the Contractor shall be responsible for obtaining analytics from the ITSM Tools, Telephony Reporting Platforms and Service Catalogues for the purposes of completing monthly Service Level Requirements (SLR) and periodic Key Performance Indicator (KPI) reporting. Analytic data obtained by the Contractor for the purposes of completing monthly Service Level Requirements (SLR) and periodic Key Performance Indicator (KPI) reporting shall be retained by the Contractor in a metrics repository provisioned by SSC for that purpose. The metrics repository shall be organized into a searchable database in chronological order from contract inception through to the end of the Contract Term. The Contractor shall partition the metrics repository into ESD and EUSD segments with the EUSD segment further partitioned into Public Service and Procurement Canada (PSPC), Health Canada (HC), Shared Services Canada (SSC), Canada School of Public Service (CSPS) and Infrastructure Canada (INFC) segments.

- **Updates to Metrics Repository**: the Contractor shall ensure that updates to the metrics repository are aligned with SLR and KPI reporting timelines. In other words, the SSC must be able reconcile SLR and KPI report content to the source information in the metrics repository immediately upon report issuance.
- **Access to Metrics Repository**: the Contractor shall provide SSC with on-line, real-time access to the metrics repository.
- **Service Level Requirements (SLR) Reporting:** the Contractor will continuously monitor and measure its performance for all Service Categories and shall measure and report the Level of Service for each Service Category for each month of the Contract Term.
- **KPI Reporting:** the Contractor shall report on Key Performance Indicators (KPIs) in a prescribed manner and frequency (i.e. daily, weekly, and monthly accumulations).
- **Report Repository**: SSC shall provide a secure common drive for storage and retention of all SLR and KPI reports. The Contractor shall be responsible for uploading and organizing reports to the common drive in accordance with the respective reporting deadlines.

2.0 Delivery Location Requirements

- **General:** The Contractor must provide and make ready for use the delivery Locations required to house ESD & EUSD contact centre resources where such facilities are compliant with the GC requirements.
- **Multiple Facilities:** The Contractor must provision and deliver services from at least 2 distinct facilities to provide service redundancy and resilience.
- **Located in Canada:** the two Contractor Facilities must be located in Canada.
- **Geographical Separation:** the two Contractor Facilities must be sufficiently geographically dispersed within Canada at a minimum distance of 200 Km so that they cannot be impacted simultaneously by adverse climatic conditions, infrastructure service disruptions (i.e. power outages), and crisis situations.
- **Service Desk Services:** the ESD and EUSD shall be accommodated in Contractor-provided and managed facilities with the distribution of personnel to be managed by the Contractor.
- **Site Inspection:** SSC shall have the right to inspect the Contractor Facilities prior to commencement of service delivery and periodically during the term Contract Term.
- **Dedicated Environment:** all Contactor Services must be accessed directly and performed within a secure and dedicated environment, independent to that of the Contractor's other environments. This will facilitate independent audits of Contractor service.

3.0 Infrastructure Requirements

- **Desktop Devices and Telephones/Headsets:** at their expense, the Contractor shall provide workstations (including operating software) and telephones/headsets for all employees, agents, sub-contractors and management of the Contractor and/or its Partner(s) (Contractor Personnel) working at the Contractor Premises. Such workstations must meet or exceed specifications set forth by SSC.
- **Desktop Applications:** at their expense, the Contractor shall ensure that current versions of the following Desktop Applications are installed on workstations used by Contractor Personnel:
    - Microsoft Windows Operating System (currently version 10)
    - Internet Explorer
    - Google Chrome
    - Mozilla Firefox
    - Citrix Receiver / Citrix Workspace
    - Third Party Second Factor Authenticator Application

- **Desktop Environment:** at their expense, the Contractor must keep their desktop environment up-to-date. The desktop software must not exceed N-1. Where N is a major release from the vendor.
- **Security Patching:** at their expense, the Contractor must apply all vendor security related patches (operating system, software installed on workstations) within 14 Federal Government Working Days (FGWD) from release and within 48 hours for all urgent/critical patches as identified by SSC.
- **Remote Access to SSC Applications and Services:** SSC will provide the Contractor with a remote access Virtual Desktop Infrastructure (VDI) solution. This solution will be accessible via the internet, providing Contractor Personnel located at the Contractor Delivery Locations with secure, managed access to the necessary tool(s), software and databases located within the Government of Canada Network (GC Net).
- **Remote Access Performance:** the VDI solution provided by SSC will offer sufficient performance and capacity to enable the Contractor to meet its service level obligations. Through the VDI, Contractor Personnel will be provided secure, managed access to GC systems and services including the HCCS, agent knowledge base and ITSM tools. SSC will provide credentials for access to all systems.
- **Infrastructure:** at their expense, the Contractor is responsible for all configuration (tweaks, drivers, or other configuration), effort and cost to enable their infrastructure to support the SSC VDI solution. The Contractor must provide and make ready for use the technical infrastructure within the Contractor Delivery Locations as required to provide Service Desk Services where such technical infrastructure includes, but is not limited to, agent telephony equipment, desktop infrastructure and the infrastructure required to interface the Contractor with the required government-provided data network services as set out in the target environment.
- **Citrix Workspace Client:** at their expense, the Contractor must provide and deliver physical desktop devices to their staff and SSC shall provide the secure desktop interface. This will take the form of a Virtual Desktop Infrastructure (VDI) provided, administered and operated by SSC. The Contractor must ensure that all desktop devices are installed with Citrix Workspace client software in order to allow Contractor Personnel to successfully establish connection to the SSC Environment.
- **Second Factor Authentication:** at their expense, the Contractor will set-up a third party second factor authenticator application. The SSC CITRIX solution, uses two-factor authentication based on RFC 6238 and supports the following list (Google authenticator (phone app), WinAuth (PC app), MS authenticator, Authy, LastPass) of two-step verification services using Time Based One-Time Password (TOTP).
- **Wide Area Network (WAN):** at their expense, the Contractor shall be responsible for the provision of resilient internet connectivity to their facilities in a configuration that aligns to the service level requirements.
- **Network Performance:** the Contractor will continuously monitor and measure their network and internet connection and provide a Network Performance Report monthly.
- **DR/BCP Connectivity:** at their expense, the Contractor shall provide connectivity required to support the DR/BCP.
- **Information Technology Service Management Tools (ITSM Tools):** The Contractor must use the ITSM Tools provided by SSC.
- **Telephony Platform(s):** the Contractor must use the Telephony Platform provided by SSC. SSC will provide a one-time training session to the Contractor on HCCS. It is the expectation that the Contractor will develop their own training material and train their personnel over the term of the contract on how to use HCCS.
- **Remote Takeover Tool(s) and Service Desk Software:** the Contractor must use the Remote Takeover Tools (EUSD only) and Service Desk Software provided by SSC.
- **Knowledge Databases:** the Contractor must use the Knowledge Database(s) provided by SSC.

4.0 Business Continuity and Disaster Recovery Requirements

- **Business Continuity:** the Contractor Delivery Locations must be (i) geographically separated (ii) use different power grids, and (iii) be served by different telecommunications service providers.
- **Minimum Fail Over:** the Contractor must commence fail over service from the back-up delivery location within two (2) hours from service disruption at the originating delivery location.
- **Minimum Fail Back:** the Contractor must commence fail back service to the originating delivery location within two (2) hours from restoration of services at the originating delivery location.
- **Disaster Recovery Plan:** the Contractor must provide SSC with a disaster recovery plan within one hundred and twenty (120) FGWDs from Contract Award.
- **Disaster Recovery Scenarios:** the Proponent's technical response shall include types of scenarios that will be addressed by their proposed disaster recovery solution.
- **Disaster Recovery Testing:** at their expense, the Contractor shall, on an annual basis with appropriate notification to SSC, test the fail-over of both facilities. Within two (2) FGWDs of the annual test, the Contractor will provide SSC with an Annual Confirmation of Disaster Recovery Testing Report detailing testing procedures undertaken and indicating the success or failure of the test. In the event of a failure, the Contractor will produce a remediation plan within ten (10) FGWDs from the test for review and approval by SSC.

5.0 Security Requirements

- **General:** The Contractor must provide and deliver Service Desk Services that meet Canada's security requirements as outlined in this document with the provisions of the Security Requirements Check List (SRCL) that is provided in this document.
- **Government of Canada Security Policies:** at their expense, the Contractor must comply with all of GC security policies and must complete the IT Security Risk Management process with a residual amount of risk acceptable to GC.
- **Security Safeguards:** the Contractor will have the appropriate safeguards on their local infrastructure. SSC will require the Contractor to elaborate on (i) what safeguards will be in place, (ii) how those safeguards will be monitored over the Contract Term, and (iii) the reporting of monitoring results. The safeguards may include, but will not be limited to the following:
    - Strong passwords of at least 12 characters with symbols, numbers and characters.
    - Firewall to protect their local network from incoming internet traffic
    - Up to date Antivirus software
    - Regular scans of the desktops for spyware
    - Software on the desktop is kept up to date
    - Ethical use of the desktops
    - Unique user accounts
- **Designated Organization Screening:** the Contractor must, at all times during the performance of the contract hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding and Production Capabilities at the level of Protected B, issued by the Canadian Industrial Security Directorate, of Public Services and Procurement Canada (CISD/PSPC).
- **Personnel Security Clearances:** all Contractor Personnel, including but not limited to full-time and part-time employees, contractors, or any other resource having access to Canada's confidential materials, systems and services must be cleared to the Reliability Status as defined by CISD/PSPC for personnel security screening.
- **Facility Security Clearance:** the Contractor must attain a Facility Security Clearance (FSC) and Document safeguarding capability (DSC) for access to information and assets of the same or lower classification level as the clearance being granted.

- **Infrastructure Security Requirements:** any and all IT systems, networks and devices of the Contractor must comply, at all times during the performance of the contract, with the CISD/PSPC security requirements for such systems, networks and devices.
- **Periodic Inspections:** On a frequency to be determined by the Safety, Security and Emergency Management Division (SSEMD) CISD/PSPC shall retain the right to conduct inspections of the Contractor IT environment and IT systems to ensure compliance with Government of Canada standards and policies with respect to the handling, storage and processing of sensitive information.
- **Access Reporting:** on a monthly basis, the Contractor must list roles and access rights on the system for all Contractor Personnel.
- **Service Management Guide:** the Contractor must provide a Service Management Guide to SSC, detailing Privacy/Security breach processes within sixty (60) FGWD from Contract Award.
- **Privacy Management Plan:** the Contractor must provide a Privacy Management Plan to SSC within sixty (60) FGWD from Contract Award. The Privacy Management Plan must be approved and acceptable to SSC, and must be maintained by the Contractor;
- **Adherence to Privacy Management Plan:** Contractor Personnel must adhere to the latest version of the Privacy Management Plan accepted by SSC.
- **Privacy Impact Assessment:** the Contractor must assist SSC in creating the Privacy Impact Assessment by providing information requested by SSC within 20 FGWDs of that request.
- **Designation:** Canada has determined that the materials accessed in the delivery of Service Desk Services have been designated up to the level of "Protected B". As defined by Canada, Protected B designation applies to information or assets that, if compromised, could cause serious injury to an individual, organization or government.
- **Limitations on Use of Personal Information:** Contractor Personnel are prohibited from the accessing, communication, transfer, disclosure, retention, processing and management of the personal information that is under the stewardship of the SSC except for the purpose of carrying out the work required under the contract.
- **Restriction on Protected Information:** the Contractor must not utilize its Information Technology systems to electronically process, produce or store Protected B information unless the CISD/PSPC has approved its use. After approval has been granted or approved, these tasks may be performed up to the level of Protected B, including an IT link up to the level of Protected B.
- **Add Hoc Reporting**: the Contractor shall report Security incident and Privacy Breaches and indicate activities undertaken to counteract the alerts and attacks.
- **Security and Privacy Reporting:** the contractor shall report, as required, to demonstrate and confirm compliance with the security and privacy requirements of Canada for provided facilities, infrastructure Service Desk Services and Contractor Personnel.
- **Security and Privacy Policies and Procedures:** The Contractor must have a clearly defined and documented set of information security and privacy policies and procedures including but not limited to:
    - Data classification, handling and privacy
    - Authentication & Access Control
    - Security and privacy training and awareness
    - Systems administration, patching and configuration
    - Information Security Incident and Privacy Breaches response
    - Regular audits and testing
    - Security and privacy requirements for the Contractor's third-party business partners and Contractors

6.0 Pricing Requirements

- **Pricing Response:** the Proponent's pricing response shall include a volume-based Monthly Variable Service Cost for each of the following initial Base Services:
    i. ESD Call/Email/Email Listener/Service Catalogue Contacts

ii. EUSD Call/Email/Service Catalogue Contacts.

SSC retains the right to add additional channels to the list of Base Services at its discretion.

- **Dead Band**: the Proponent's pricing response shall include a Dead Band at +/- 5% of Monthly Baseline Service Volumes (to be provided by SSC).
- **ARCs/RRCs**: the Proponent's pricing response shall include an ARC unit rate for actual Service Volumes experienced above the Upper Dead Band Limit for three consecutive months and an RRC unit rate for actual Service Volumes experienced below the Lower Dead Band Limit for three consecutive months.
- **Upset Limit**: actual Service Volumes experienced at >20% above the Monthly Service Volume Baseline for three consecutive months, or >20% below the Monthly Service Volume Baseline will require renegotiation of the Service Volume Baseline, Monthly Variable Service Cost and ARCs/RRCs.
- **Service Level Credits:** failure to meet Minimum Service Level(s) in a given month shall result in a Service Level Credit applied against amounts owed by SSC to the Contractor in the month.
- **Earn Back Entitlement:** the Contractor shall be entitled to earn back the Service Level Credit for consistent performance at or above the Minimum Service Level(s) in subsequent months.

7.0 Conditions Precedent – Prior to Signing

- **Physical Access Controls:** prior to contract signing, the Proponent must demonstrate that requisite Physical Access Controls are currently in place, or show a plan and timeline (acceptable to SSC) to have them in place by commencement of service delivery.
- **Data Privacy (Protected B):** prior to contact signing, the Proponent must demonstrate that requisite Data Privacy Controls are currently in place, or show a plan and timeline (acceptable to SSC) to have them in place by commencement of service delivery.

8.0 Transition

- **General:** The Contractor must transition Service Desk Services from the current service delivery model, facilities and infrastructure to the Contractor provided Service Desk Services to meet the transition requirements and timelines.
- **Language Proficiency:** during transition, and prior to service commencement, the Contractor must provide an organization chart and documented procedures demonstrating how the Contractor shall achieve and maintain compliance with bilingual proficiency requirements for the duration of the Contract Term.
- **Personnel:** during transition, and prior to service commencement, the Contractor must provide a plan demonstrating how the Contractor will source and retain qualified personnel in sufficient quantity to meet Minimum Service Levels for the duration of the Contract Term.
- **Transition Activities:** In order to facilitate timely management and implementation of the transition effort the Core Project Team resources dedicated to the transition efforts must be either located in the National Capital Region, or be able to meet/shadow/work extensively in person with SSC and its current contractor at its current locations in the NCR.
- **Telephony Platform Training:** SSC will provide a onetime training session to the Contractor on the Telephony Platform. It is the expectation that the Contractor will develop their own training material and train their personnel over the term of the contract on how to use the Telephony Platform.

9.0 On-going

- **General**: The Contractor must provide and deliver the requested Service Desk Services through the operating model that addresses the requirements. The Contractor must, as and when requested, provide other Service Desk related services that may include but are not limited to enhanced service analytics, support for new or additional contact modalities, ad-hoc reporting, or other Service Desk related services such as delivery, planning, management or administration services.
- **Collaboration:** the Contractor must enable Contractor resources to work closely with SSC staff in-person or remotely in order to facilitate flexible and responsive communications and collaborative work processes, and to minimize non-productive travel time.

ANNEX A – STATEMENT OF WORK

Table of Contents

Schedule A 1 – Service Desk Services

Shared Services Canada (SSC)

Schedule A 1 – Service Desk Services

Table of Contents

List of Tables

Schedule A 1 – Service Desk Services

This Statement of Work and all its attachments form part of the Agreement between SHARED SERVICES CANADA (SSC) and [SUPPLIER'S LEGAL NAME] dated MONTH, DAY, 2020, and are governed by the terms and conditions of that Agreement.

1.0 Service Desk Services Overview and Service Objectives

1.1 Service Desk Services Overview

Shared Services Canada (SSC) is responsible for delivering mandated email, telecommunications, data centre and network services to Partner Departments and limited services to Client Agencies/Organizations in a consolidated and standardized manner to support the delivery of Government of Canada (GC) programs and services.

As part of its mandate, SSC provides enterprise infrastructure service desk support to Partner Departments through the Enterprise Service Desk. Offering service 24 hours a day, 7 days a week, and 365 days a year including all holidays, the Enterprise Service Desk (ESD) provides bilingual desk-to-desk infrastructure support for issues relating to SSC-mandated services.

SSC provides optional end-user service desk service to Partner GC departments ("End User Customers"). SSC currently provides bilingual, end-user support to five End User Customers (including SSC) for incident reporting and request fulfillment relating to desktop environments (encompassing applications and technology) utilized by 36,000+ end-users. For greater clarity, this is not a desk-to-desk model.

This Schedule sets forth the roles and responsibilities that the Contractor must perform for the ESD and End User Service Desk (EUSD) Services provided under the Contract as part of the Service Desk Services.

Service Desk Services include the services and activities, as further detailed in this Schedule, required to coordinate and respond to Incidents, Service Requests and Change Requests made by supported customers (**see Schedule A 12 – Customers Supported**).

The Service Desk Services must include the following, as a minimum:

a. Provision of a single point of contact (SPOC) for all Incidents Reports and Service Requests.

b. Support to Problem Management (PM) activities and PM integration, including proactive trend analysis of Incidents and overall reduction in the number of Incidents over time, as documented in **Schedule A 2 – Service Management Services**;

c. Support to Change Management activities, as and when required, as documented in **Schedule A 10 - Policies and Procedures**;

d. Request Fulfillment for Service Requests consistent with procedures documented in **Schedule A 10 - Policies and Procedures**;

e. Service Request Fulfillment, for all Partner Service Desk Agents;

f. Service Request Fulfillment and Incident Reporting for End-user devices, including desktops, laptops, notebooks, tablets and other in-scope devices;

g. Support of self-service functionality for common requests as agreed with SSC, particularly as related to the SSC Service Catalogue;

h. Innovation in and leveraging of new/emerging technologies, including integration with existing tools and achieving defined Service Level targets, which may progressively increase over time (**Schedule B 2 - Service Level Requirements**); and

i. Provision of pre-defined higher service levels to VIP (Very Important Person) end-users (**Schedule B 2 - Service Level Requirements**).

1.2 Service Objectives

The following are the key high-level Service objectives SSC expects to achieve through fully managed Enterprise and End User Service Desk Services as represented in the Statement of Work (SOW):

a. Improve Client Satisfaction to the fullest extent possible across all aspects of Enterprise and End User Support Services through faster speed-to-answer/respond, higher resolution upon first contact, lower abandonment rates and improved Average Handle Time using existing Client Satisfaction results as a baseline;

b. Improve SSC efficiency and effectiveness by adopting Contractor-leveraged best practices in the areas of client reporting, logging, and Fulfilment of Service Requests and Resolution of IT Incidents;

c. Acquire, as necessary, skilled Service Desk support for new technologies early in their life cycle while maintaining support for older technologies;

d. Establish redundant managed service site locations;

e. Reduce agent turnover and retain skills/knowledge in Service Desk operations;

f. Enhance Disaster Recovery (DR) and Business Continuity Plans (BCP) for all client groups, leveraging the Contractor's capabilities within the scope of the Statement of Work;

g. Ensure cost-effective delivery of service;

h. Establish an agile/scalable delivery model to meet changing demand;

i. Continuously improve service metrics and performance through automated capabilities such as analytics and machine learning to improve overall service quality; and

j. Offer multiple "channels of choice" to accommodate current user preferences; and

k. Optimize self-service opportunities.

1.3 Schedules

The Contractor must maintain up-to-date versions of the Schedules referred to in this section. However, any change to the content of the Schedules outlined below must reflect a change permitted under this Agreement and/or be approved by SSC. Updated versions of the Schedules will not form part of this Statement of Work. The Contractor must make any such updated documents available to SSC on a quarterly basis.

Following are the Schedules currently included with this **Schedule A 1 – Service Desk Services** Statement of Work:

- Schedule A 2 – Service Management Services;
- Schedule A 3 – Transition Services;
- Schedule A 4 – Governance and Relationship Management Services;
- Schedule A 5 – High-Level Design with Security Controls;
- Schedule A 6 – Security Requirements Traceability Matrix;
- Schedule A 7 – Glossary; Definition of Key Terms;
- Schedule A 8 – System and Network Architecture;
- Schedule A 9 – Organization Structure;
- Schedule A 10 – Policies and Procedures;
- Schedule A 11 – Timing of Reporting and Events
- Schedule A 12 – Customers Supported;
- Schedule A 13 – Types of Contacts Handled;
- Schedule A 14 – Service Desk Workload Baseline;
- Schedule A 15 – Privacy;
- Schedule A 16 – Professional Services;
- Schedule B 1 – Pricing Provisions;

- Schedule B 2 – Service Level Requirements;
- Schedule B 3 – Financial Responsibility Matrix; and
- Schedule B 4 – Reporting.

2.0 Service Environment

Schedule A 2 – Service Management Services outlines the schedules that describe the service environment for all in-scope services to be supported and/or with which the Contractor must comply. The following further describes the service environment to be supported in relation to this Schedule.

2.1 Enterprise Service Desk (ESD)

Using a desk-to-desk model the ESD is the first point of contact for all Partner Service Desks. The ESD Service Desk Service involves the Fulfilment of Service Requests as well as Incident Reporting and Change Management, which includes ticket creation, escalation, and resolution wherever possible. The ESD serves as the national escalation point of contact for all in-scope tickets from Partner Service Desks. The Service Desks also provides a single point-of-contact on the status of incidents, problems and change requests.

Currently the primary contact methods are toll-free numbers, email and on-line portal with the potential of expanding to other contact channels as technologies become available.

2.1.1 ESD Customers Supported

The Contractor must support all ESD Customers defined in **Schedule A 12 – Customers Supported**.

2.1.2 ESD Types of Contacts to be Handled

The Contractor must resolve, escalate or dispatch all contacts. Types of contacts and their expected disposition are detailed in **Schedule A 13 – Types of Contacts Handled**.

2.1.3 ESD IT Service Lines Encompassed

The ESD provides desk-to-desk infrastructure support for issues relating to SSC mandated services (email, telecommunications, data centre and network services to supported Customers).

2.1.4 ESD Operating Hours

The Contractor must provide support services to ESD Customers 24 hours a day, 7 days a week, and 365 days a year including all holidays.

2.1.5 ESD Language Requirements

The Enterprise Service Desk must provide support services to users in the official language of their choice. Those support services, including all written and verbal communications, must be of equal quality and level of service in English and French, at all times.

2.1.6 ESD Hardware, Software, Telephony Platforms, Tools and Knowledge Database

SSC and the Contractor shall be responsible for provisioning of the ESD in accordance with **Schedule B 3 - Financial Responsibility Matrix**. Hardware, software, telephony platform, tools and the knowledge database shall be provisioned as follows:

2.1.7 ESD Hardware, Software and Telephones

At their expense, the Contractor shall provide workstations, operating software and telephones/headsets for all employees, agents and sub-contractors, as well as management of the Contractor and/or its Partner(s) (Contractor Personnel) working at the Contractor Premises. Such workstations must meet or exceed specifications set forth by SSC.

At their expense, the Contractor must apply all vendor security related patches for operating system and applications installed on workstations within 14 Federal Government Working Days (FGWD) from release and within 48 hours for all urgent/critical patches as identified by SSC.

2.1.8 ESD Desktop Applications

At their expense, the Contractor shall ensure that current versions of the Desktop Applications (as detailed in **Schedule B 3 – Financial Responsibility Matrix**). At their expense, the Contractor must keep their desktop environment up-to-date. The desktop software must not exceed N-1, where N is a major release from the software vendor.

2.1.9 ESD ITSM Tool(s) / Service Desk Software / Knowledge Databases

SSC will provide the Contractor with a remote access Virtual Desktop Infrastructure (VDI) solution. This solution will be accessible via the internet, providing Contractor Personnel located at the Contractor Premises with secure, managed access to the necessary tool(s), software and databases located within the Government of Canada Network (GC Net). The VDI solution provided by SSC will offer sufficient performance and capacity to enable the Contractor to meet their service-level obligations.

At their expense, the Contractor is responsible for all configuration (tweaks, drivers, appropriate operating system version or other configuration), effort and cost to enable their infrastructure to support the SSC VDI solution. The Contractor must provide and make ready for use the technical infrastructure within the Contractor facilities as required to provide Service Desk Services, where such technical infrastructure includes, but is not limited to, agent telephony equipment and desktop infrastructure and the infrastructure required to interface the Contractor with the required government-provided data network services, as set out in the target environment. In addition, the contractor shall be responsible for the provision of resilient internet connectivity to their facilities in a configuration that aligns to the service level requirements.

Multiple Service Desk Applications are used by the ESD in support of ESD Customers. The Contractor will be required to use the Service Desk Applications provided by SSC (see **Section 1** of **Schedule B 3 – Financial Responsibility Matrix**) and it is expected that all agents will be trained in the use of these Service Desk Applications. The Service Desk Applications provided by SSC are subject to change at SSC's discretion.

2.1.10 ESD Telephony Platform

The Contractor must use the Hosted Contact Centre Service (HCCS) Telephony Platform provided by SSC. HCCS enables Departments/Agencies to interact with external and internal GC clients efficiently, effectively, and economically. Clients can contact Departments/Agencies using traditional telephony (PSTN, Centrex, PBX, or mobile) and alternate contact channels such as Voice over Internet Protocol (VoIP), email, text messaging, video, and social media. HCCS provides the infrastructure required by Departments/Agencies to create and to run their own contact centres. This infrastructure is virtual (cloud-based) and requires minimal infrastructure on premises: End User Devices (EUD) for agents, supervisors and managers, and connectivity. The Telephony Platform provided by SSC is subject to change at SSC's discretion.

2.2 End User Service Desk (EUSD)

The EUSD operates five Service Desks supporting the desktop environments for five customer departments. The EUSD Service Desk Service includes the Fulfilment of Service Requests as well as Incident Reporting. The End User Service Desk agents are dedicated to their specific customer with cross-training between SSC and PSPC.

Currently the primary contact method is by local/toll-free number (see **Schedule A 12 – Customers Supported**) with the potential of expanding to other contact channels as technologies become available.

2.2.1 EUSD Customers Supported

The Contractor must support all EUSD Customers defined in **Schedule A 12 – Customers Supported**.

2.2.2 EUSD Types of Contacts to be Handled

The Contractor must resolve, escalate or dispatch all contacts. Types of contacts and their expected disposition are detailed in **Schedule A 13 – Types of Contacts Handled**.

2.2.3 EUSD IT Service Lines Encompassed

The EUSD provides end-user support to supported Customers (including SSC) for incident management and request fulfillment relating to desktop environments (encompassing applications and technology).

2.2.4 EUSD Operating Hours

The Contractor must provide support services to EUSD Customers during the following operating hours:

Table 1: EUSD Operating Hours

	Customer Name [Department]	Core Business Hours	Saturdays and Sundays	Federal Statutory Holidays
1.	Public Services and Procurement Canada	06:00 – 21:00 E.T.	09:00 – 17:00 E.T.	N/A
2.	Health Canada	07:00 – 20:00 E.T.	N/A	N/A
3.	Shared Services Canada	06:00 – 20:00 E.T.	N/A	N/A
4.	Canada School of Public Service	06:00 – 20:00 E.T.	N/A	N/A
5.	Infrastructure Canada	07:00 – 17:00 E.T.	N/A	N/A

Hours of operation are subject to change based on business requirements and direction from SSC. SSC and the Contractor shall review and agree on any changes to the operating hours.

2.2.5 EUSD Language Requirements

The EUSD must provide support services to users in the official language of their choice. Those support services, including all written and verbal communications, must be of equal quality and level of service in English and French, at all times.

2.2.6 EUSD Hardware, Software, Telephony Platforms, Tools and Knowledge Database

SSC and the Contractor shall be responsible for provisioning of the EUSD in accordance with **Schedule B 3 - Financial Responsibility Matrix**. Hardware, software, telephony platform, tools and the knowledge database shall be provisioned as follows:

2.2.6.1 EUSD Hardware, Software and Telephones

At their expense, the Contractor shall provide workstations, operating software and telephones/headsets for all employees, agents and sub-contractors, as well as management of the Contractor and/or its Partner(s) (Contractor Personnel) working at the Contractor Premises. Such workstations must meet or exceed specifications set forth by SSC.

At their expense, the Contractor must apply all vendor security related patches for operating system and applications installed on workstations within 14 Federal Government Working Days (FGWD) from release and within 48 hours for all urgent/critical patches as identified by SSC.

2.2.6.2 EUSD Desktop Applications

At their expense, the Contractor shall ensure that current versions of the Desktop Applications (as detailed in **Schedule B 3 – Financial Responsibility Matrix**). At their expense, the Contractor must keep their desktop environment up-to-date. The desktop software must not exceed N-1, where N is a major release from the software vendor.

2.2.6.3 EUSD ITSM Tool(s) / Service Desk Software / Knowledge Databases

SSC will provide the Contractor with a remote access Virtual Desktop Infrastructure (VDI) solution. This solution will be accessible via the internet, providing Contractor Personnel located at the Contractor Premises with secure, managed access to the necessary tool(s), software and databases located within the Government of Canada Network (GC Net). The VDI solution provided by SSC will offer sufficient performance and capacity to enable the Contractor to meet their service level obligations.

At their expense, the Contractor is responsible for all configuration (tweaks, drivers, appropriate operating system version or other configuration), effort and cost to enable their infrastructure to support the SSC VDI solution. The Contractor must provide and make ready for use the technical infrastructure within the Contractor facilities as required to provide Service Desk Services, where such technical infrastructure includes, but is not limited to, agent telephony equipment and desktop infrastructure and the infrastructure required to interface the Contractor with the required government-provided data network services, as set out in the target environment. In addition, the contractor shall be responsible for the provision of resilient internet connectivity to their facilities in a configuration that aligns to the Service Level Requirements.

Multiple Service Desk Applications are used by the EUSD in support of EUSD Customers. The Contractor will be required to use the Service Desk Applications provided by SSC (see **Section 2** of **Schedule B 3 – Financial Responsibility Matrix**) and it is expected that all agents will be trained in the use of these Service Desk Applications. The Service Desk Applications provided by SSC are subject to change at SSC's discretion.

2.2.6.4 EUSD Telephony Platform

The Contractor must use the Hosted Contact Centre Service (HCCS) Telephony Platform provided by SSC. HCCS enables Departments/Agencies to interact with external and internal GC clients efficiently, effectively, and economically. Clients can contact Departments/Agencies using traditional telephony (PSTN, Centrex, PBX, or mobile) and alternate contact channels such as Voice over Internet Protocol (VoIP), email, text messaging, video, and social media. HCCS provides the infrastructure required by Departments/Agencies to create and to run their own contact centres. This infrastructure is virtual (cloud-based) and requires minimal infrastructure on premises: End User Devices (EUD) for agents, supervisors and managers, and connectivity. The Telephony Platform provided by SSC is subject to change at SSC's discretion.

2.3 Projects

The Contractor must execute and complete certain projects that are either in-flight or planned. Such projects are the responsibility of the Contractor to complete as part of the Transition activities (**Schedule A 3 – Transition Services**) and as required during the life of the Contract (**Schedule A 4 - Governance and Relationship Management Services**) in accordance with timeframes specified by SSC.

2.4 System and Network Architecture

A reference System and Network Architecture for the integration between SSC-provided tools/telephony and the EUSD and ESD is detailed in **Schedule A 8 – System and Network Architecture**.

2.5 Organization Structure

SSC Organization Charts for the Department, Sector, Directorate and unit responsible for Service Desk and Request Fulfilment are included in **Schedule A 9 – Organization Structure**.

2.6 Policies and Procedures

The Contractor must comply with all relevant GC, SSC and other relevant departmental Policies and Procedures, including, but not limited to, those identified in **Schedule A 10 – Policies and Procedures**. For greater certainty, specific Privacy requirements are identified in **Schedule A 15 – Privacy**.

2.7 Events and Reporting

A summary of milestone events and reporting obligations is provided in **Schedule A 11 – Schedule of Events and Reporting.**

2.8 Contractor Delivery Locations

2.8.1 General

The Contractor must provide and make ready for use the two facilities required to accommodate ESD & EUSD Contractor Personnel where such facilities are compliant with the GC requirements.

2.8.2 Multiple Delivery Locations

The Contractor must deliver the Service Desk Services from at least 2 distinct facilities to provide service redundancy and resilience.

2.8.3 Located in Canada

The two Contractor Facilities must be located in Canada.

2.8.4 Geographical Separation

The two Contractor Facilities must be sufficiently geographically dispersed within Canada at a minimum distance of 200 Km so that they cannot be impacted simultaneously by adverse climatic conditions, infrastructure service disruptions (i.e. power outages), and crisis situations.

2.8.5 Service Desk Services

The ESD and EUSD shall be accommodated in Contractor-provided and managed facilities with the distribution of personnel to be managed by the Contractor.

2.8.6 Site Inspection

SSC shall have the right to inspect the Contractor Facilities prior to commencement of service delivery and periodically during the term Contract Term.

2.8.7 Dedicated Environment

All Contactor Services must be accessed directly and performed within a secure and dedicated environment, independent to that of the Contractor's other environments. This will facilitate independent audits of Contractor service.

2.9 Business Continuity and Disaster Recovery

2.9.1 Business Continuity

The Contractor Facilities must be (i) geographically separated (ii) use difference power grids, and (iii) be served by different telecommunications service providers.

2.9.2 Disaster Recovery

The Contractor shall provide cross-training of ESD and EUSD agents to enable each desk to operate as a disaster recovery site for the other.

2.9.3 Minimum Fail Over

The Contractor must commence fail over service from the back-up facility within two (2) hours from service disruption at the originating facility.

2.9.4 Minimum Fail Back

The Contractor must commence fail back service to the originating facility within two (2) hours from restoration of services at the facility.

2.9.5 Disaster Recovery Plan

The Contractor must provide SSC with a disaster recovery plan within 120 FGWDs from Contract Award.

2.9.6 Disaster Recovery Scenarios

The Proponent's technical response shall include types of scenarios that will be addressed by their proposed disaster recovery solution.

2.9.7 Disaster Recovery Testing

At their expense, the Contractor shall, on an annual basis with appropriate notification to SSC, test the fail-over of both Contractor Facilities. Within 2 FGWD of the annual test, the Contractor will provide SSC with an Annual Confirmation of Disaster Recovery Testing Report detailing testing procedures undertaken and indicating the success or failure of the test. In the event of a failure, the Contractor will produce a remediation plan within 10 FGWD from the date of the test for review and approval by SSC.

2.10 Service Desk Baseline Information

SSC current Service Desk utilization and projected usage is provided in **Schedule A 14 – Service Desk Workload Baseline**. These business requirements represent SSC's most realistic projection of the Service requirements based on a combination of past trends and current anticipated overall business direction over the Term of the Contract.

3.0 Service Descriptions and Roles and Responsibilities

The Contractor must provide the following Level 1 Service Desk Services.

In all tables in this section, an "X" is placed in the column named "Contractor" to indicate that the Contractor must perform the task. The Contractor is not required to perform the task where an "X" is placed in the column "SSC".

3.1 Enterprise Service Desk (ESD) Services

3.1.1 ESD General Roles and Responsibilities

The following table identifies the General roles and responsibilities that the parties must perform.

Table 2: ESD General Roles and Responsibilities

Identifier	General Service Roles and Responsibilities	Contractor	SSC
2.01	Define Service Desk Operations requirements and policies.		X
2.02	Develop, document and maintain Service Desk Operations procedures and processes that meet SSC requirements and adhere to SSC policies.	X	
2.03	Review and approve Service Desk Operations procedures.		X
2.04	Identify, resolve where possible and escalate reported Incidents.	X	
2.05	Manage Incident Resolution and Close Incidents, including those escalated to Third Parties.		X
2.06	Manage Service Request creation and/or Resolution and close any such Service Requests as required.	X	
2.07	Provide appropriately trained Service Desk staff for Level 1 remote support to meet the SSC requirements.	X	
2.08	Coordinate the Root Cause Analysis process on re-occurring High and Critical Incidents.		X

Identifier	General Service Roles and Responsibilities	Contractor	SSC
2.09	Provide multilingual support as required by SSC.	X	
2.10	Coordinate with Support Groups, Partner Service Desks and Third Parties and external agencies for Incident Resolution and Root Cause Analysis (RCA).		X
2.11	Identify changes in processes required for improvement purposes.	X	
2.12	Track tickets start to end, identify any bouncing between groups, SLA misses and timely escalation.		X
2.13	Drive continuous improvement of achieved Service Levels and KPI's etc.	X	
2.14	Create various trend analysis reports.	X	
2.15	Develop training material; deliver training to new members and staff on tools, processes and methods from time to time; and provide SSC access to training materials.	X	
2.16	Based on feedback from the Contractor, drive intelligent automation and analytics to implement predictive, proactive, preventive and prescriptive capabilities to deal with day-to-day operations.		X
2.17	Maintain or improve knowledge database accuracy and effectiveness in order to carry out and comply with any SSC operationally driven changes and/or requirements.	X	
2.18	Perform modifications to maintain or improve knowledge database efficiency and effectiveness.		X
2.19	Recommend functional and informational changes to the ITSM tool(s) in order to improve overall use of the ITSM tool(s) and performance of the Service Desk and the information passed on to support groups.	X	
2.20	Make resources available, at any time of the day and week potentially on very short notice, to work with the technical authority to restore regular service in case of major system and environmental problems, such as: natural disaster, virus, etc. Make resources available, at any time of the day and week potentially on very short notice, to work with the technical authority to: i. Restore regular service in case of major system and environmental problems, such as: natural disaster, virus, etc. ii. At the discretion of the Technical Authority, provide resources in the delivery of ad-hoc activities. The types of resources are described in Schedule A 16 – Professional Services. The rates for these resources is included in Annex B – Basis of Payment.	X	
2.21	Create policies with respect to business continuity for critical Service Desk functions and systems.		X
2.22	Develop contingency plan for critical Service Desk functions and systems.	X	
2.23	Approve contingency plan for critical Service Desk functions and systems.		X
2.24	Test and execute contingency plans for critical Service Desk functions and systems.	X	
2.25	Maintain inventory of pre-recorded phone system emergency messages to ensure currency and accuracy.	X	
2.26	Implement inventory of pre-recorded phone system emergency messages into HCCS.	X	
2.27	Record emergency broadcast phone system messages live in both official languages when a message is required and when no appropriate pre-recorded message exists, following SSC Standards.	X	
2.28	Record new phone system wait queues and voice mail messages to reflect any changes in procedure.	X	
2.29	Recommend changes to the telephony system script or other functions to enhance performance or meet new procedural requirements.	X	
2.30	Work collaboratively with SSC for the implementation and testing of all approved changes.	X	

Identifier	General Service Roles and Responsibilities	Contractor	SSC
2.31	Implement tools necessary to provide Service Desk Services and meet SSC informational and functional requirements.		X
2.32	Configuration and management of ITSM Tool(s).		X
2.33	Design, develop and document manual or backup procedures for Service Desk personnel to follow in the event that the Service Desk tools used to process Partner Service Desk Agent contacts fail to operate properly.		X
2.34	Implement manual or backup procedures for Service Desk personnel to follow in the event that the Service Desk tools used to process Partner Service Desk Agent contacts fail to operate properly.	X	
2.35	Document escalation procedures to be followed in the event that Service Desk personnel are unable to perform any/part of their job functions because of system, communication, application availability, or other Contractor site-related problems.	X	
2.36	Review / provide feedback on escalation procedures.		X
2.37	Report any security breaches (including, but not limited to malware, unauthorized access, viruses etc.) to the appropriate authority according to procedure.	X	
2.38	Communicate and work with the Security group to remain informed on any security issue.	X	

3.1.2 ESD Single Point of Contact (SPOC) Service

Single Point of Contact Services for all Partner Service Desks. The ESD Service Desk Service involves the fulfilment of service requests as well as incident management and change management, which includes ticket creation, escalation, and resolution wherever possible.

Table 3: ESD SPOC Roles and Responsibilities

Identifier	Single Point of Contact Service Roles and Responsibilities	Contractor	SSC
3.01	Define Single Point of Contact (SPOC) Services requirements and policies.		X
3.02	Develop, document and maintain SPOC procedures and processes that meet SSC requirements and adhere to SSC policies.	X	
3.03	Review and approve SPOC procedures.		X
3.04	Provide Agent Phone sets / Headsets.	X	
3.05	Provide software and equipment (e.g., Interactive Voice Response [IVR], Automatic Call Distribution [ACD]) needed to collect, track and manage Service Requests and Service Incidents received over the phone by the Service Desk.		X
3.06	Provide SPOC call-in access via assigned global toll-free numbers for all Service Desk Services.		X
3.07	Provide SPOC for all Incident Reports.	X	
3.08	Provide SPOC for all Service Requests for information and Service (e.g., IMACs) in the Service Lines supported under this SOW.	X	
3.09	Provide multiple alternative communications channels, including voice messages, email, instant messaging, social media, virtual face-to-face (video chat or web conferencing), Chat-bots and intranet.		X
3.10	Integrate new communications channels into standard operating processes.	X	
3.11	Record and transfer (i.e., call responsible party or enter ticket) out-of-scope Service Line Incidents and Service Requests based on scripts or other direction from Client.	X	
3.12	Provide peer-to-peer (P2P) support for working with peers from respective business units for assistance.	X	
3.13	Implement knowledge management tools and methodologies for mining the existing knowledge database and link it with automation framework for automated or manual access.		X

3.1.3 ESD Service Desk Operations and Administration Service

Service Desk Operations and Administration Services are the activities associated with providing a stable Service Desk environment and to effectively and efficiently perform procedures to ensure Service Desk Services meet Service Level Requirements. The following table identifies the Service Desk Operations and Administration roles and responsibilities that the parties must perform.

Table 4: ESD Service Desk Operations and Administration Service Roles and Responsibilities

Identifier	Service Desk Operations and Administration Service Roles and Responsibilities	Contractor	SSC
4.01	Define Service Desk Operations and Administration Services requirements and policies.		X
4.02	Develop, and document and maintain Service Desk Operations and Administration Services procedures that meet requirements and adhere to defined policies.	X	
4.03	Review and approve Service Desk Operations and Administration Services procedures.		X
4.04	Provide escalation contact list(s) for Partner Service Desk Agent contacts.		X
4.05	Develop escalation process including quarterly validation.		X
4.06	Maintain and provide escalation contact list(s) for all Service Lines (including Third Parties such as Suppliers and Service Suppliers).		X
4.07	Review and approve escalation process.		X
4.08	Issue broadcasts or other notices to provide status updates as required for planned and unplanned events.	X	
4.09	Provide Partner Service Desk Agent online/portal access to Service Requests and Incident Reports based on SSC criteria.		X
4.10	Provide Partner Service Desk Agent online access to view/display ticket status based on SSC criteria.		X
4.11	Develop procedures for conducting Partner Service Desk Agent Satisfaction Surveys in accordance with the Service-Level Requirements.	X	
4.12	Review and approve procedures for conducting Partner Service Desk Agent Satisfaction Surveys.		X
4.13	Execute procedures for conducting Partner Service Desk Agent Satisfaction Surveys.	X	
4.14	Maintain a continuous improvement program that improves Service Desk Service delivery.	X	
4.15	Review client satisfaction surveys and customer feedback and propose corrective action(s) (i.e. update documentation, address performance concerns, callback customer, etc.) in response to unsatisfactory feedback.	X	
4.16	Approve corrective action(s) to be taken.		X
4.17	Execute corrective action(s) to be taken.	X	
4.18	Work with other Service Suppliers operational and technical staff and SSC to identify solutions that minimize the need to call the Service Desk (e.g., additional Partner Service Desk Agent training, self-help support opportunities, Root Causes Analysis).	X	
4.19	Review and approve solutions that minimize the need to call the Service Desk through more self-serve capabilities and "How To" manuals		X
4.20	Coordinate and make available environment documentation (i.e., network configuration and inventory of applications to be supported).		X
4.21	Perform analytics of data in real-time and identify service improvement opportunities.	X	
4.22	Provide additional Resources, as needed, during planned and unplanned critical events, potentially on very short notice.	X	
4.23	Track/manage/report Service Desk utilization and prepare trend analyses.	X	

3.1.4 ESD Request Fulfilment Service

Service Request Fulfilment Services are the activities associated with end-to-end Service Request processes, including assignment/escalation to resolver groups through a defined process, including the Contractor's primary resources; Third Parties, such as equipment and software suppliers, other Third Parties such as authorized representatives in SSC's client departments, and SSC internal technical support resources. The following table identifies the Request Fulfilment Service roles and responsibilities that the parties must perform.

Table 5: ESD Request Fulfilment Service Roles and Responsibilities

Identifier	Request Fulfilment Service Roles and Responsibilities	Contractor	SSC
5.01	Define Service Request Management Service requirements and policies.		X
5.02	Develop, document and maintain Service Request Service procedures, including procedures to receive and respond to Service Request Contacts according to defined prioritization targets that meet SSC requirements and adhere to SSC policies.	X	
5.03	Review and approve Service Request procedures.		X
5.04	Identify and describe priorities, response and resolution targets for Service Requests that have differing impacts.		X
5.05	Provide a system to document, manage and track all Service Requests, and inquiries regardless of the means by which the Service Request is submitted (e.g., telephone, email, fax and direct online input by End-Users).		X
5.06	Categorize, prioritize and log all Service Request Tickets in the ITSM Tool(s).	X	
5.07	Actively monitor all Service Requests and ensure appropriate action is taken according to procedures and prescribed thresholds.	X	
5.08	Verify acceptance of Services by contacting the Partner Service Desk Agent to confirm results and level of satisfaction.	X	
5.09	Verify that all records (e.g., inventory, asset and Configuration Management records) are updated to reflect completed/resolved Service Request (e.g., IMACs).	X	
5.10	Provide authorization to the process of closing Service Requests.		X
5.11	Send Service Requests closure notices, per Client policies.	X	
5.12	Provide insights and processes to establish Level 0 (self-help) resources.	X	
5.13	Provide materials and guidance to support education/training of Partner Service Desk Agents to drive more self-service and preventive measures.	X	
5.14	Educate/train Partner Service Desk Agents to drive more self-service and preventive measures.		X

3.1.5 ESD Incident Reporting Service

Incident Reporting Services are the activities associated with the logging, triage, and assignment of reported incidents to resolver groups through a defined process, including the Contractor's primary resources; Third Parties, such as equipment and software suppliers, other Third Parties such as authorized representatives in SSC's client departments, and SSC internal technical support resources. The following table identifies the Incident Reporting Service roles and responsibilities that the parties must perform.

Table 6: ESD Incident Management Service Roles and Responsibilities

Identifier	Incident Reporting Service Roles and Responsibilities	Contractor	SSC
6.01	Define Incident Reporting Service requirements and policies.		X
6.02	Develop, document and maintain Incident Management Service procedures, including procedures to receive and respond to Incident Management Contacts according to defined prioritization and	X	

Identifier	Incident Reporting Service Roles and Responsibilities	Contractor	SSC
	resolution targets that meet SSC requirements and adhere to SSC policies.		
6.03	Review and approve Incident Reporting procedures.		X
6.04	Identify and describe priorities, response and resolution targets for Incidents that have differing impacts.		X
6.05	Use SSC ITSM tool(s) to document, categorize, prioritize and assign all Incidents.	X	
6.06	Identify, resolve where possible and escalate reported Incidents.	X	
6.07	Provide end-to-end Incident Resolution (management) and closure, including incidents escalated to Third Parties.		X
6.08	Monitor unresolved Incidents and manage tickets via ITIL end-to-end Incident Management.		X
6.09	Actively monitor all calls, incident, problems, and change management tickets for status, and ensure the appropriate action is taken according to procedures and prescribed thresholds.		X
6.10	Document solutions to Resolved Incidents in knowledge database.		X
6.11	Ensure that recurring Incidents are reviewed using RCA processes.		X
6.12	Verify that all records (e.g., inventory, asset and Configuration Management records) are updated to reflect completed/resolved Incidents.		X
6.13	Send Service Desk Incident closure notices, per Client policies.	X	
6.14	Provide insights and processes to establish Level 0 (self-help) resources.	X	
6.15	Track repetitive incidents and escalate such cases to the appropriate teams to take corrective measures along with suggestions, if any.		X
6.16	Track RCAs and ensure that problem ticket has been captured against the Incidents that require a full-fledged RCA. For all other Incidents, ensure that cause of Incident has been captured, at a minimum.		X
6.17	Provide materials and guidance to support education/training of Partner Service Desk Agents to drive more self-service and preventive measures.		X
6.18	Educate/train Partner Service Desk Agents to drive more self-service and preventive measures.		X
6.19	Participate in Incident, Problem and Change Management review sessions with SSC.	X	

3.1.6 ESD Change Management Service

The following table identifies the Change Management Service roles and responsibilities that the parties must perform.

Table 7: ESD Change Management Service Roles and Responsibilities

Identifier	Change Management Service Roles and Responsibilities	Contractor	SSC
7.01	Validate the request and ensure the proper information has been obtained from the SSC Representative.	X	
7.02	Perform checking of the necessary IT environment for change management such as requests for change and account administration aspects to ensure client service is uninterrupted.	X	
7.03	Perform initial validation of change management request and translate / tailor the request using the correct template.	X	
7.04	Record all details of the request per pre-defined templates.	X	
7.05	Classify the Request for Change (RFC) and determine the change model.	X	
7.06	Assign the RFC to the appropriate service groups.	X	
7.07	Monitor the RFCs requesting status updates and updating the request.	X	
7.08	Define change management process and task workflows.		X
7.09	Inform appropriate support groups of issues related to a change request, and escalate any issues to the relevant group(s).	X	

Identifier	Change Management Service Roles and Responsibilities	Contractor	SSC
7.10	Ensure work performed is accounted for and required action are taken to respect the request.	X	

3.1.7 ESD Application Service

Application Services are the activities associated with identifying the various tasks of the Contractor and SSC for dealing with application-related Incidents and Requests. The following table identifies Service Desk application services roles and responsibilities that the parties must perform.

Table 8: ESD Application Service Roles and Responsibilities

Identifier	Application Service Roles and Responsibilities	Contractor	SSC
8.01	Create process and procedures for providing first-level support for Application Services.	X	
8.02	Resolve Partner Service Desk Agent queries by providing required information from Service Desk.	X	
8.03	Assign tickets to correct resolver groups in Application Services.	X	
8.04	Create and track account creation SRs for access to application.	X	
8.05	Revoke application access during employee exits or role changes.	X	
8.06	Maintain access profiles of Partner Service Desk Agents, and generate reports on various access provided to Partner Service Desk Agents.	X	

3.1.8 ESD Self-Help Support Service

Self-Help Support Services are the activities associated with IVR capabilities, voice messaging with guaranteed call-back responses, intranet-based automated self-help support, etc. The following table identifies the Self-Help Support Service roles and responsibilities that the parties must perform.

Table 9: ESD Self-Help Support Service Roles and Responsibilities

Identifier	Self-Help Service Roles and Responsibilities	Contractor	SSC
9.01	Define Self-Help Support Service requirements and policies.		X
9.02	Develop, document and maintain Self-Help Support Service Contractor procedures that meet Client requirements and adhere to Client policies.	X	
9.03	Review and approve Self-Help Support Service procedures.		X
9.04	Implement Self-Help Support Service capabilities, which enable Partner Service Desk Agents to perform self-service, "How To" support through Partner Service Desk Agent access to knowledge databases, and online Incident status checking.	X	
9.05	Monitor and report on the effectiveness of Self-Help Support Service capabilities and usage.	X	
9.06	Develop and provide recommendations for improvements to Self-Help Support Service capabilities.	X	
9.07	Review and approve recommendations for improvements to Self-Help Support Service capabilities.		X
9.08	Implement approved recommendations for improvements to Self-Help Support Service capabilities.	X	
9.09	Improve and upgrade Self-Service processes to align with new requirements and to improve customer experience.	X	
9.10	Provide self-help capability.		X
9.11	Provide content for Self-Help, such as online FAQs and help documentation for common issues across the Service Desk, based on a review of service requests and incidents.	X	
9.12	Assist with improvements to the self-help capability.	X	
9.13	Keep Authorized Users regularly updated with alerts advising of any new or changed information on events or as requested.	X	

Identifier	Self-Help Service Roles and Responsibilities	Contractor	SSC
9.14	Deliver communications plans and education for new or changes to self-service facilities, subject to approval.	X	

3.1.9 ESD Exception Requests Service

Exception Requests Services are the activities associated with fulfilling Enterprise User requests for products or Services that are outside the scope of the Services. The following table identifies the Exception Requests Service roles and responsibilities that the parties must perform.

Table 10: ESD Exception Requests Service Roles and Responsibilities

Identifier	Exception Requests Service Roles and Responsibilities	Contractor	SSC
10.01	Define Exception Request Service policies and requirements.		X
10.02	Develop, document and maintain Exception Request Service process, procedures and required forms that meet SSC requirements and adhere to SSC policies.	X	
10.03	Review and approve Contractor Exception Request Service procedures.		X
10.04	Document Exception Requests in the ITSM Tool(s), collect and analyze the request, recommend Exception Request action, and advise the originator of the status.	X	
10.05	Review and approve Exception Requests.		X
10.06	Take the necessary action to implement the Request, as long as the Exception is within scope of this Contract or an approved project.	X	
10.07	Provide Exception Request status to requestor when approved.	X	

3.1.10 ESD Planning and Analysis Service

Planning and Analysis Services are the activities associated with providing SSC the most appropriate and effective level of Service on an ongoing basis. The following table identifies Planning and Analysis Service roles and responsibilities that the parties must perform.

Table 11: ESD Planning and Analysis Service Roles and Responsibilities

Identifier	Planning and Analysis Service Roles and Responsibilities	Contractor	SSC
11.01	Identify and recommend Service Desk solution that best meets SSC business needs and service-level expectations on an ongoing basis.	X	
11.02	Review and approve recommended Service Desk solutions.		X
11.03	Perform operational planning for Service Desk capacity and performance purposes.	X	
11.04	Perform analysis of SSC environment, including acquiring SSC management team feedback, to identify the appropriate sets of skills, training and experience needed by Service Desk staff.	X	
11.05	Define of technical parameters of Service Desk tools, portal and ITSM tool (system architecture, operational parameter).	X	
11.06	Analyze call volumes and ramp-up and ramp-down resources based on efficiency gained and increase/decrease of demand.	X	
11.07	Plan and create a roadmap for increasing Service Desk efficiency to reduce the number of calls per user per month.	X	
11.08	Continuously scan the market for available best practice and update the processes and engage with client to incorporate new capabilities.	X	
11.09	Explore how the Service Desk can drive further business performance for SSC, propose and provide approved innovative approaches for using Service Desk capabilities to increase business outcome and performance.	X	
11.10	Review and approve innovative approaches and implementations.		X

3.1.11 ESD Service Desk Reporting Service

Service Desk Reporting Services are the activities associated with the preparation of and access to Service Desk reports that are based on defined criteria. The following table identifies Service Desk Reporting Service roles and responsibilities that the parties must perform.

The Contractor must provide at a minimum the set of reports included in **Schedule B 4 – Reporting**.

Table 12: ESD Service Desk Reporting Service Roles and Responsibilities

Identifier	Service Desk Reporting Service Roles and Responsibilities	Contractor	SSC
12.01	Recommend a list of Service Desk management reports.	X	
12.02	Review, recommend and approve list of Service Desk management reports.		X
12.03	Report on Service Desk statistics and trends (e.g., Service Request volumes and trends by types, ESD Customer, product etc.).	X	
12.04	Report on trends in Service Requests indicating a need for training.	X	
12.05	Audit report results and Service Desk operations periodically.		X
12.06	Ad hoc reporting by ESD Customer.	X	
12.07	Forecast and trend analysis reports.	X	

3.1.12 ESD Service Desk IVR/ACD Support Service

Interactive Voice Response (IVR) and Automatic Call Distribution (ACD) Services are those required to respond to voice calls from the Client(s) that are related to specific call types that have predetermined instructions. The Contractor must provide these capabilities to improve productivity, ensure consistent communication and resolution to Incidents and Service Requests. The following table identifies Service Desk IVR/ACD Support Service roles and responsibilities that the parties must perform.

Table 13: ESD Service Desk IVR/ACD Support Service Roles and Responsibilities

Identifier	Service Desk IVR/ACD Support Service Roles and Responsibilities Service	Contractor	SSC
13.01	Define, implement and manage an IVR/ ACD process.		X
13.02	Suggest configuration of IVR/ACD and help in testing the call flow through the system.	X	
13.03	Forecast capacity requirements of IVR/ACD.		X
13.04	Ensure availability as per SLA for call centre equipment, including IVR/ACD, and implement necessary systems for call handling.		X
13.05	Provide global toll-free numbers for end-user access.		X

3.1.13 ESD Business Value and Innovation Management Support Service

Business Value and Innovation Management Support Services analyzes Incidents and Service Requests to identify and support the resolution and/or elimination of business-related IT problems. Business Value Management is about supporting the business in the context of IT support. The following table identifies Business Value and Innovation Management Support Service roles and responsibilities that the parties must perform.

Table 14: ESD Business Value and Innovation Management Roles and Responsibilities

Identifier	Business Value and Innovation Management Support Service Roles and Responsibilities	Contractor	SSC
14.01	Capture, manage and analyze technical and business-specific knowledge.	X	
14.02	Capture knowledge based on Incidents and Service Requests, as logged and/or otherwise captured by the Contractor.	X	

Identifier	Business Value and Innovation Management Support Service Roles and Responsibilities	Contractor	SSC
14.03	Identify areas for improvement in IT Support, Processes and Tooling based on captured knowledge.	X	
14.04	Nominate a Business Value Manager as part of Contractor Service operations to manage and operate the Contractor Business Value Management process.	X	
14.05	Present the output of the Contractor analysis and improvement to the respective Governance Committees.	X	
14.06	Support rules based on reconciled business data to prioritize Incidents.	X	
14.07	Support rules based on reconciled business data to prioritize Service Requests.	X	
14.08	Provide and implement at least one innovative or new idea in every quarter that either impacts business or IT Operations positively from a cost, experience, and business impact or efficiency perspective.	X	

3.2 End-User Service Desk (EUSD) Services

3.2.1 EUSD General Roles and Responsibilities

The following table identifies the General roles and responsibilities that the parties must perform.

Table 15: EUSD General Roles and Responsibilities

Identifier	General Service Roles and Responsibilities	Contractor	SSC
15.01	Define Service Desk Operations requirements and policies.		X
15.02	Develop, document and maintain Service Desk Operations procedures and processes that meet SSC requirements and adhere to SSC policies.	X	
15.03	Review and approve Service Desk Operations procedures.		X
15.04	Provide expert Level 1 assistance for inquiries about the features, functions and usage of hardware and software.	X	
15.05	Identify, resolve where possible and escalate reported Incidents.	X	
15.06	Manage Incident Resolution and Close Incidents, including those escalated to Third Parties.		X
15.07	Manage Service Request creation and/or Resolution and close any such Service Requests as required.	X	
15.08	Provide appropriately trained Service Desk staff for Level 1 remote support to meet the SSC requirements.	X	
15.09	Coordinate the RCA process on re-occurring High and Critical Incidents.		X
15.10	Provide multilingual support as required by SSC.	X	
15.11	Coordinate with Support Groups, Partner Service Desks and Third Parties and external agencies for Incident Resolution and RCA.		X
15.12	Identify changes in processes required for improvement purposes.	X	
15.13	Track tickets start to end, identify any bouncing between groups, SLA misses and timely escalation.		X
15.14	Drive continuous improvement of achieved Service Levels and KPI's etc.	X	
15.15	Create various trend analysis reports.	X	
15.16	Develop training material; deliver training to new members and staff on tools, processes and methods from time to time; and provide SSC access to training materials.	X	
15.17	Based on feedback from the Contractor, drive intelligent automation and analytics to implement predictive, proactive, preventive and prescriptive capabilities to deal with day-to-day operations.		X
15.18	Maintain or improve knowledge database accuracy and effectiveness in order to carry out and comply with any SSC operationally driven changes and/or requirements.	X	

Identifier	General Service Roles and Responsibilities	Contractor	SSC
15.19	Perform modifications to maintain or improve knowledge database efficiency and effectiveness.		X
15.20	Recommend functional and informational changes to the ITSM tool(s) in order to improve overall use of the ITSM tool(s) and performance of the Service Desk and the information passed on to support groups.	X	
15.21	Make resources available, at any time of the day and week potentially on very short notice, to work with the technical authority to restore regular service in case of major system and environmental problems, such as: natural disaster, virus, etc. Make resources available, at any time of the day and week potentially on very short notice, to work with the technical authority to: i. Restore regular service in case of major system and environmental problems, such as: natural disaster, virus, etc. ii. At the discretion of the Technical Authority, provide resources in the delivery of ad-hoc activities. The types of resources are described in Schedule A 16 – Professional Services. The rates for these resources is included in Annex B – Basis of Payment.	X	
15.22	Create policies with respect to business continuity for critical Service Desk functions and systems.		X
15.23	Develop contingency plan for critical Service Desk functions and systems.	X	
15.24	Approve contingency plan for critical Service Desk functions and systems.		X
15.25	Test and execute contingency plans for critical Service Desk functions and systems.	X	
15.26	Maintain inventory of pre-recorded phone system emergency messages to ensure currency and accuracy.	X	
15.27	Implement inventory of pre-recorded phone system emergency messages into HCCS.	X	
15.28	Record emergency broadcast phone system messages live in both official languages when a message is required and when no appropriate pre-recorded message exists, following SSC Standards.	X	
15.29	Record new phone system wait queues and voice mail messages to reflect any changes in procedure.	X	
15.30	Recommend changes to the telephony system script or other functions to enhance performance or meet new procedural requirements.	X	
15.31	Work collaboratively with SSC for the implementation and testing of all approved changes.	X	
15.32	Implement tools necessary to provide Service Desk Services and meet SSC informational and functional requirements.		X
15.33	Configuration and management of ITSM Tool(s).		X
15.34	Design, develop and document manual or backup procedures for Service Desk personnel to follow in the event that the Service Desk tools used to process Partner Service Desk Agent contacts fail to operate properly.		X
15.35	Implement manual or backup procedures for Service Desk personnel to follow in the event that the Service Desk tools used to process Partner Service Desk Agent contacts fail to operate properly.	X	
15.36	Document escalation procedures to be followed in the event that Service Desk personnel are unable to perform any/part of their job functions because of system, communication, application availability, or other Contractor site-related problems.	X	
15.37	Review / provide feedback on escalation procedures.		X
15.38	Report any security breaches such as, but not limited to, reports of viruses to the appropriate authority according to procedure.	X	
15.39	Communicate and work with the Security group to remain informed on any security issue.	X	

3.2.2 EUSD Single Point of Contact (SPOC) Service

Single Point of Contact Services provide toll-free end-user support and electronic ticketing for logging, tracking, resolution and reporting of Service Desk Incidents and Service Requests for desktop environments for five End User Customers. The following table identifies the SPOC roles and responsibilities that the parties must perform.

Table 16: EUSD SPOC Roles and Responsibilities

Identifier	Single Point of Contact Service Roles and Responsibilities	Contractor	SSC
16.01	Define Single Point of Contact (SPOC) Services requirements and policies.		X
16.02	Develop, document and maintain SPOC procedures and processes that meet SSC requirements and adhere to SSC policies.	X	
16.03	Review and approve SPOC procedures.		X
16.04	Provide Agent Phones/Headsets.	X	
16.05	Provide software and equipment (e.g., Interactive Voice Response [IVR], Automatic Call Distribution [ACD]) needed to collect, track and manage Service Requests and Service Incidents received over the phone by the Service Desk.		X
16.06	Provide SPOC call-in access via assigned global toll-free numbers for all Service Desk Services.		X
16.07	Provide SPOC and coordination for all Incident Reports.	X	
16.08	Provide SPOC and coordination for all Service Requests for information and Service (e.g., IMACs) in the Service Lines supported under this SOW.	X	
16.09	Provide multiple alternative communications channels, including voice messages, email, instant messaging, social media, virtual face-to-face (video chat or web conferencing), Chat-bots and intranet.		X
16.10	Integrate new communications channels into standard operating processes.	X	
16.11	Record and transfer (i.e., call responsible party or enter ticket) out-of-scope Service Line Incidents and Service Requests based on scripts or other direction from SSC.	X	
16.12	Provide peer-to-peer (P2P) support for working with peers from respective business units for assistance.	X	
16.13	Implement knowledge management tools and methodologies for mining the existing knowledge and link it with automation framework for automated or manual access.		X

3.2.3 EUSD Service Desk Operations and Administration Service

Service Desk Operations and Administration Services are the activities associated with providing a stable Service Desk environment and to effectively and efficiently perform procedures to ensure Service Desk Services meet Service Level Requirement (SLR) targets and requirements. The following table identifies the Service Desk Operations and Administration roles and responsibilities that the parties must perform.

Table 17: EUSD Service Desk Operations and Administration Service Roles and Responsibilities

Identifier	Service Desk Operations and Administration Service Roles and Responsibilities	Contractor	SSC
17.01	Define Service Desk Operations and Administration Services requirements and policies.		X
17.02	Develop, and document and maintain Service Desk Operations and Administration Services procedures that meet requirements and adhere to defined policies.	X	
17.03	Review and approve Service Desk Operations and Administration Services procedures.		X
17.04	Provide escalation contact list(s) for end-user contacts.		X
17.05	Develop escalation process including quarterly validation.		X

Identifier	Service Desk Operations and Administration Service Roles and Responsibilities	Contractor	SSC
17.06	Maintain and provide escalation contact list(s) for all in-scope Service Lines (including Third Parties such as Suppliers and Service Suppliers).		X
17.07	Review and approve escalation process.		X
17.08	Issue broadcasts or other notices to provide status updates as required for planned and unplanned events.	X	
17.09	Provide end-user online/portal access to Service Requests and Incident Reporting.		X
17.10	Provide end-user online access to view/display incident status.		X
17.11	Develop procedures for conducting End-User Satisfaction Surveys in accordance with the Service-Level Requirements.	X	
17.12	Review and approve procedures for conducting End-User Satisfaction Surveys.		X
17.13	Execute procedures for conducting end-user Satisfaction Surveys.	X	
17.14	Maintain a continuous improvement program that improves Service Desk Service delivery.	X	
17.15	Review end-user Satisfaction surveys and end-user feedback and propose corrective action(s) (i.e. update documentation, address performance concerns, callback customer, etc.) in response to unsatisfactory feedback.	X	
17.16	Approve corrective action(s) to be taken.		X
17.17	Execute corrective action(s) to be taken.	X	
17.18	Work with other Service Suppliers' operational and technical staff and the Client to identify solutions that minimize the need to call the Service Desk (e.g., additional end-user training, self-help support opportunities, RCA).	X	
17.19	Review and approve solutions that minimize the need to call the Service Desk through more self-serve capabilities and "How To" manuals.		X
17.20	Coordinate and make available environment documentation (i.e., network configuration and inventory of software to be supported).		X
17.21	Perform analytics of data in real-time and identify service improvement opportunities.	X	
17.22	Provide additional Resources, as needed, during planned and unplanned critical events, potentially on very short notice.	X	
17.23	Track/manage/report Service Desk utilization and prepare trend analyses.	X	

3.2.4 EUSD Request Fulfilment Service

Service Request Fulfilment Services are the activities associated with end-to-end Service Request processes, including escalation to Level 2 and Level 3 specialists through a defined process, including the Contractor's primary resources; Third Parties, such as equipment and software suppliers, other Third Parties such as authorized representatives in SSC's client departments, and SSC internal technical support resources. The following table identifies the Request Fulfilment Service roles and responsibilities that the parties must perform.

Table 18: EUSD Request Fulfilment Service Roles and Responsibilities

Identifier	Request Fulfilment Service Roles and Responsibilities	Contractor	SSC
18.01	Define Service Request Management Service requirements and policies.		X
18.02	Develop, document and maintain Service Request Service procedures, including procedures to receive and respond to Service	X	

Identifier	Request Fulfilment Service Roles and Responsibilities	Contractor	SSC
	Request Contacts according to defined prioritization targets that meet SSC requirements and adhere to SSC policies.		
18.03	Review and approve Service Request procedures.		X
18.04	Provide a system to document, manage and track all Service Requests, and inquiries regardless of the means by which the Service Request is submitted (e.g., telephone, email, fax and direct online input by End-Users).		X
18.05	Categorize, prioritize and log all Service Request Tickets in the ITSM Tool(s).	X	
18.06	Actively monitor service request tickets for status and ensure the appropriate action is taken according to procedures and prescribed thresholds.	X	
18.07	Verify acceptance of Services by contacting the end-user to confirm results and level of satisfaction.	X	
18.08	Verify that all records (e.g., inventory, asset and Configuration Management records) are updated to reflect completed/resolved Service Request (e.g., IMACs).	X	
18.09	Provide authorization to the process of closing Service Requests.		X
18.10	Send Service Requests closure notices, per Client policies.	X	
18.11	Provide insights and processes to establish Level 0 (self-help) resources.	X	
18.12	Provide materials and guidance to support education/training of end-users to drive more self-service and preventive measures.	X	
18.13	Educate/train end-users to drive more self-service and preventive measures.		X

3.2.5 EUSD Incident Reporting Service

Incident Reporting Services are the activities associated with the logging, triage, and assignment of reported incidents to resolver groups through a defined process, including the Contractor's primary resources; Third Parties, such as equipment and software suppliers, other Third Parties such as authorized representatives in SSC's client departments, and SSC internal technical support resources. The following table identifies the Incident Reporting Service roles and responsibilities that the parties must perform.

Table 19: EUSD Incident Reporting Service Roles and Responsibilities

Identifier	Incident Reporting Service Roles and Responsibilities	Contractor	SSC
19.01	Define Incident Reporting Service requirements and policies.		X
19.02	Develop, document and maintain Incident Reporting Service procedures, including procedures to receive and respond to Incident Reporting Contacts according to defined prioritization and resolution targets that meet SSC requirements and adhere to SSC policies.	X	
19.03	Review and approve Incident Reporting procedures.		X
19.04	Identify and describe priorities, response and resolution targets for Incidents that have differing impacts.		X
19.05	Use SSC ITSM tool(s) to document, manage and track all Incidents.	X	
19.06	Identify, resolve where possible and escalate reported Incidents.	X	
19.07	Provide end-to-end Incident identification, escalation, resolution (management) and closure, including incidents escalated to Third Parties.		X
19.10	Monitor unresolved Incidents and manage tickets via ITIL end-to-end Incident Management.		X
19.11	Actively monitor all incident tickets for status and ensure the appropriate action is taken according to procedures and prescribed thresholds.		X

Identifier	Incident Reporting Service Roles and Responsibilities	Contractor	SSC
19.12	Troubleshoot Incidents using the Service Contractor knowledge databases and/or Third-Party knowledge databases.	X	
19.13	Resolve Incidents at Level 1 if possible, otherwise escalate in accordance with documented procedures.	X	
19.14	Resolve incidents on first call in accordance with documented procedures.	X	
19.15	Document solutions to Resolved Incidents in knowledge database.		X
19.18	Ensure that recurring Incidents are reviewed using RCA processes.		X
19.19	Verify that all records (e.g., inventory, asset and Configuration Management records) are updated to reflect completed/resolved Incidents.		X
19.20	Provide authorization to the process of closing Service Desk Incidents.		X
19.21	Send Service Desk Incident closure notices, per Client policies.	X	
19.22	Provide insights and processes to establish Level 0 (self-help) resources.	X	
19.23	Track repetitive incidents and escalate such cases to the appropriate teams to take corrective measures along with suggestions, if any.		X
19.24	Track RCAs and ensure that problem ticket has been captured against the Incidents that require a full-fledged RCA. For all other Incidents, ensure that cause of Incident has been captured, at a minimum.		X
19.25	Assist End Users with questions relating to functionality and use of in-scope equipment and software.	X	
19.26	Provide materials and guidance to support education/training of end-users to drive more self-service and preventive measures.		X
19.27	Educate/train end-users to drive more self-service and preventive measures.		X
19.28	Participate in Incident, Problem and Change Management review sessions with SSC.	X	

3.2.6 EUSD Remote Device Takeover Service

Remote Device Takeover Services are the activities associated with managing, maintaining and troubleshooting devices remotely over the network to minimize the need to dispatch technical personnel for Incident Resolution. The following table identifies the Remote Device Takeover Service roles and responsibilities that the parties must perform.

Table 20: EUSD Remote Device Takeover Service Roles and Responsibilities

Identifier	Remote Device Takeover Service Roles and Responsibilities	Contractor	SSC
20.01	Define Service Desk Remote Device requirements and policies.		X
20.02	Develop, document and maintain Remote Device Takeover Service procedures that meet requirements and adhere to defined policies and security requirements.	X	
20.03	Review and approve Remote Device Takeover Service procedures.		X
20.04	Resolve Incidents using remote-control capability and, when possible, implement corrective actions. If resolution is not possible, escalate using established escalation procedures.	X	
20.05	Provide remote control tool		X
20.06	Utilize remote control tools to manage and enforce compliance with standards.	X	
20.07	Develop competencies and capabilities in resolving incidents associated with remote devices and impart such training from time to time on tools and techniques.	X	

3.2.7 EUSD Application Service

Application Services roles and responsibilities identify the various tasks associated with the Contractor and SSC for dealing with application-related Incidents and Requests. The following table identifies the Application Service roles and responsibilities that the parties must perform.

Table 21: EUSD Application Service Roles and Responsibilities

Identifier	Application Service Roles and Responsibilities	Contractor	SSC
21.01	Create process and procedures for providing first-level support for Application Services.	X	
21.02	Provide Service Desk training and Level 1 scripts for in-scope applications software on the approved list.	X	
21.03	Resolve end-user queries by providing required information from Service Desk.	X	
21.04	Assign tickets to correct resolver groups in Application Services.	X	
21.05	Create and track account creation SRs for access to application.	X	
21.06	Revoke application access during employee exits or role changes as directed by SSC.	X	
21.07	Maintain access profiles of end-users, and generate reports on various access provided to end-users.	X	

3.2.8 EUSD End-User Administration Service

End-User Administration Services are the activities associated with managing and coordinating account creation, activation, termination, Changes and expiration. The following table identifies the End-User Administration Services roles and responsibilities that the parties must perform.

***Table 22: EUSD* End-User Administration Service Roles and Responsibilities**

Identifier	End-User Administration Service Roles and Responsibilities	Contractor	SSC
22.01	Define End-User Administration Services requirements and policies.		X
22.02	Develop, document and maintain End-User Administration Service procedures that meet SSC requirements and adhere to SSC policies.	X	
22.03	Review and approve End-User Administration Service procedures.		X
22.04	Receive, track and process requests for end-user account creation/activation, changes and terminations.	X	
22.05	Coordinate end-user account administration, creation/activation, changes and terminations (e.g., password/account setup and password reset, remote access connectivity, email accounts, and end-user IDs).	X	
22.06	Create, change and delete end-user accounts per requests, in accordance with SSC security policies.	X	
22.07	Coordinate as necessary with other specialized areas to manage end-user accounts.		X
22.08	Perform password resets as required, in accordance with the SSC's security policies.	X	
22.09	Coordinate implementation of cognitive automation capabilities to solve end-user incidents by driving agentless capabilities.		X
22.10	Build analytics capabilities to drive operational efficiency, identify potential hotspots, and analyze trends and forecasts.		X
22.11	Track assets and inventory for licenses, and escalate any discrepancies.	X	
22.12	Upon request, provide reporting on all accesses assigned to End-User, service and system accounts.	X	
22.13	Provide reporting capabilities to support audit and compliance requirements (ability to audit the requests and approvals).	X	

3.2.9 EUSD Self-Help Support Service

Self-Help Support Services are the activities associated with provisioning of a self-help portal for users to make service requests and resolve simple incidents. The following table identifies the Self-Help Support Service roles and responsibilities that the parties must perform.

***Table 23: EUSD* Self-Help Support Service Roles and Responsibilities**

Identifier	Self-Help Service Roles and Responsibilities	Contractor	SSC
23.01	Define Self-Help Support Service requirements and policies.		X
23.02	Develop, document and maintain Self-Help Support Service Contractor procedures that meet SSC requirements and adhere to SSC policies.	X	
23.03	Review and approve Self-Help Support Service procedures.		X
23.04	Implement Self-Help Support Service capabilities, which enable end-users to perform self-service, "How To" support through end-user access to knowledge bases, and online Incident status checking.	X	
23.05	Monitor and review the effectiveness of Self-Help Support Service capabilities and usage.		X
23.06	Develop and provide recommendations for improvements to Self-Help Support Service capabilities.	X	
23.07	Review and approve recommendations for improvements to Self-Help Support Service capabilities.		X
23.08	Implement approved recommendations for improvements to Self-Help Support Service capabilities.	X	
23.09	Improve and upgrade Self-Help Service processes to align with new requirements and to improve customer experience.	X	
23.10	Provide self-help capability.		X
23.11	Provide content for Self-Help, such as online FAQs and help documentation for common issues across the Service Desk, based on a review of service requests and incidents.	X	
23.12	Assist with improvements to the self-help capability.	X	
23.13	Keep authorized users regularly updated with alerts advising of any new or changed information on events or as requested.	X	
23.14	Develop communications plans and education for new or changes to Self-Help Service facilities.	X	
23.15	Approve and execute communications plans and education for new or changes to Self-Help Service facilities.		X

3.2.10 EUSD Exception Requests Service

Exception Requests Services are the activities associated with fulfilling end-user requests for products or services that are outside the scope of the Services. The following table identifies the Exception Requests Service roles and responsibilities that the parties must perform.

***Table 24: EUSD* Exception Requests Service Roles and Responsibilities**

Identifier	Exception Requests Service Roles and Responsibilities	Contractor	SSC
24.01	Define Exception Request Service policies and requirements.		X
24.02	Develop, document and maintain Exception Request Service process, procedures and required forms that meet Client requirements and adhere to Client policies.	X	
24.03	Review and approve Service Contractor Exception Request Service procedures.		X
24.04	Document Exception Requests in the ITSM Tool(s), collect and analyze the Request, recommend Exception Request action, and advise the originator of the status.	X	
24.05	Review and approve Exception Requests.		X
24.06	Take the necessary action to implement the Request, as long as the Exception is within scope of this Contract or an approved project.	X	
24.07	Provide Exception Request status to requestor when approved.	X	

3.2.11 EUSD Planning and Analysis Service

Planning and Analysis Service are the activities associated with providing SSC the most appropriate and effective level of Service on an ongoing basis. The following table identifies the Planning and Analysis Service roles and responsibilities that that the parties must perform.

***Table 25: EUSD* Planning and Analysis Service Roles and Responsibilities**

Identifier	Planning and Analysis Service Roles and Responsibilities	Contractor	SSC
25.01	Identify and recommend Service Desk solution that best meets SSC's business needs and service-level expectations on an ongoing basis.	X	
25.02	Review and approve recommended Service Desk solutions.		X
25.03	Perform operational planning for Service Desk capacity and performance purposes.	X	
25.04	Perform analysis of the SSC environment, including acquiring SSC management team feedback, to identify the appropriate sets of skills, training and experience needed by Service Desk staff.	X	
25.05	Definition of technical parameters of Service Desk tools, portal and ITSM tool (system architecture, operational parameter).		X
25.06	Plan and create a roadmap for increasing Service Desk efficiency to reduce the number of calls per user per month.	X	
25.07	Continuously scan the market for available best practices and update the processes and engage with SSC to incorporate new capabilities.	X	
25.08	Explore how the Service Desk can drive further business performance for SSC, propose and provide approved innovative approaches for using Service Desk capabilities to increase business outcome and performance.	X	
25.09	Review and approve innovative approaches and implementations.		X

3.2.12 EUSD Service Desk Reporting Service

Service Desk Reporting Services are the activities associated with the preparation of and access to Service Desk reports that are based on defined criteria. The following table identifies Service Desk Reporting Service roles and responsibilities that the parties must perform.

The Contractor must provide at a minimum the set of reports included in **Schedule B 4 – Reporting**.

***Table 26: EUSD* Service Desk Reporting Service Roles and Responsibilities**

Identifier	Service Desk Reporting Service Roles and Responsibilities	Contractor	SSC
26.01	Recommend a list of Service Desk management reports.	X	
26.02	Review and approve list of Service Desk management reports.		X
26.03	Report on Service Desk statistics and trends (e.g., Service Request volumes and trends by types of end-users) in accordance with approved list of reports.	X	
26.04	Report on trends in Service Requests indicating a need for training.	X	
26.05	Audit report results and Service Desk operations periodically.		X
26.06	Ad hoc reporting by EUSD Customers.	X	
26.07	Forecast and trend analysis reports.	X	

3.2.13 EUSD Service Desk IVR/ACD Support Service

Interactive Voice Response (IVR) and Automatic Call Distribution (ACD) Services are those required to respond to voice calls from the Client(s) that are related to specific call types that have predetermined instructions. The Contractor must provide these capabilities to improve productivity, ensure consistent communication and resolution to Incidents and Service Requests. The following table identifies Service Desk IVR/ACD Support Service roles and responsibilities that the parties must perform.

Table 27: EUSD Service Desk IVR/ACD Support Service Roles and Responsibilities

Identifier	Service Desk IVR/ACD Support Service Roles and Responsibilities Service	Contractor	SSC
27.01	Define, implement and manage an IVR/ ACD process.		X
27.02	Suggest configuration of IVR/ACD and help in testing the call flow through the system.	X	
27.03	Forecast capacity requirements of IVR/ACD.		X
27.04	Ensure availability as per SLA for call centre equipment, including IVR/ACD, and implement necessary systems for call handling.		X
27.05	Provide global toll-free numbers for end-user access.		X

3.2.14 EUSD Business Value and Innovation Management Support Service

Business Value and Innovation Management Support Services analyzes Incidents and Service Requests to identify and support the resolution and/or elimination of business-related IT problems. Business Value Management is about supporting the business in the context of IT support. The following table identifies Business Value and Innovation Management Support Service roles and responsibilities that the parties must perform.

Table 28: EUSD Business Value and Innovation Management Roles and Responsibilities

Identifier	Business Value and Innovation Management Support Service Roles and Responsibilities	Contractor	SSC
28.01	Capture, manage and analyze technical and business-specific knowledge.	X	
28.02	Capture knowledge, based on Incidents and Service Requests, as logged and/or otherwise captured by the Contractor.	X	
28.03	Business data will be used to identify areas for improvement in IT Support, Processes and Tooling.	X	
28.04	Nominate a Business Value Manager as part of Contractor Service operations to participate in Transition to manage and operate the Contractor Business Value Management process.	X	
28.05	Present the output of the Contractor analysis and improvement to the respective Governance Committees.	X	
28.06	Support rules based on reconciled business data to prioritize Incidents.	X	
28.07	Support rules based on reconciled business data to prioritize Service Requests.	X	
28.08	Provide and implement at least one innovative or new idea in every quarter that either impacts business or IT Operations positively from a cost, experience, and business impact or efficiency perspective.	X	

3.3 Exclusions

There are no Exclusions.

4.0 Service Level Management

4.1 Service Level Requirements (SLRs)

The Contractor must meet the minimum service levels contained in **Schedule B 2 – Service Level Requirements** by the end of the Transition Period.

4.2 Service Level Reporting

The Contractor must adhere to the SLA reporting requirements contained in **Schedule B 2 – Service Level Requirements** by the end of the Transition Period.

4.3 Service Level Credits and Earn Back Opportunities

Service Level credits and earn-back opportunities associated with failures to meet minimum service levels will be calculated in accordance with **Schedule B 2 – Service Level Requirements**.

Schedule A 2 – Service Management Services

Shared Services Canada (SSC)

Schedule A 2 – Service Management Services

Table of Contents

List of Tables

Schedule A 2 – Service Management Services

1.0 Service Management Services Overview and Objectives

1.1 Service Management Services Overview

This document sets forth the roles and responsibilities of the Contractor for the Service Management Services provided under the Contract. Service Management Services are the common services and processes that apply to the provisioning, delivery and management of Service Desk Services.

Service Desk Services are the SSC Service Lines applicable to this Contract. As described in **Schedule A 7 – Glossary; Definition of Key Terms**, a "Service Line" is an IM-IT sub-organization within the SSC Enterprise that has the responsibility to plan, implement, monitor and support a line of services. The Enterprise, in this context, can comprise SSC, the Contractor and/or other Third-Party support organizations.

The in-scope Service Lines within the Contract are End User Service Desk Services and Enterprise Service Desk Services, with Service Management Services a supporting function to both Service Lines.

The services included in **Schedule A 4 – Governance and Relationship Management Services** represent a supporting service function to the Service Desk Service Lines throughout the life of the contract.

The services defined in **Schedule A 3 – Transition Services** deliver a project which ensures the Service Desk Services and Service Management Services achieve Service Launch, and at the end of the Contract, deliver a project which ensures successful Service termination and transfer.

1.2 Service Objectives

SSC expects to achieve the following high-level Service objectives through Service Management Services, which the Contractor must deliver:

- Ensure that all IT life-cycle and Service Management functions and processes are performed for the in-scope Service Lines;
- Deliver Services that support an end-to-end enterprise and life-cycle process across all in-scope Service Lines; and
- Ensure that process improvements result in improved value to SSC, which is defined as optimized overall cost of Service Desk Services at the business level and/or improved competitive capability versus industry / market trends.

2.0 Service Environment

2.1 Scope of the Service Environment to be Supported

The following subsections and related Schedules further describe and scope the End User Service Desk (EUSD) and Enterprise Service Desk (ESD) environments to be supported and/or with which the Contractor must comply. The Schedules apply to all in-scope services, including those described in Schedules: **A 1 – Service Desk Services; A 2 – Service Management Services; A 3 – Transition Services;** and **A 4 – Governance and Relationship Management Services**.

2.1.1 Hardware and Software

Hardware and software asset provisioning and support/maintenance responsibilities of the Contractor and SSC are defined in **Schedule B 3 – Financial Responsibility Matrix**.

2.1.2 System and Network Architecture

Descriptions of the Service Desk Services system and network architectures for EUSD and ESD are provided in **Schedule A 8 – System and Network Architecture**.

2.1.3 Organization Structure

The SSC organization structure as it pertains to Service Desk Services is provided in **Schedule A 9 – Organization Structure**.

2.1.4 Work In Progress

a) EUSD Migration from Service Manager 7 to Service Manager 9.

b) ESD Migration from ICE (telephony system) to new HCCS.

c) ESD Migration from ECD ITSM Tool (IBM) to BMC Remedy ITSM Tool.

2.1.5 Future Initiatives

a) Migration to a new cloud-based email system.

2.1.6 Policies and Procedures

Policies, procedures and standards compliance requirements for the Service Desk Services Contractor are delineated in **Schedule A 10 – Policies and Procedures**.

2.1.7 Personnel

The Contractor must provide resources with the necessary skills and certifications to deliver the requirements documented in Section 3.0 below and the Service Level Requirements documented **in Schedule B 2 – Service Level Requirements**.

2.1.8 Required Languages

Service Desk Services must provide support services to users in the official language of their choice. Those support services, including all written and verbal communications, must be of equal quality and level of service in English and French, at all times.

2.1.9 Maintaining Service Environment Documentation

2.1.9.1 Service Delivery Manual (SDM)

The SDM documents the scope of work, influencing factors, functional relationships, workload metrics and the actual documentation used. The Contractor must update the SDM as necessary or at a minimum every three months and provide it to the designated SSC Manager for approval and distribution within SSC. The document is an all-encompassing overview of the details of the Service Desk Services Contract. It includes, but is not limited to, the following:

- Service Desk Scope and Description;
- Service Provider / Service Desk Service Organization Chart;
- Governance Model;
- Service Desk Services Functional Description;
- Service Desk Services Relationships Diagram;
- Resourcing Plan;
- Reporting Requirements;
- Service Desk Services Responsibility Matrix;
- Communication Protocol;
- Service Desk Services Documentation;
- Shift Coverage;
- Service Desk Services Contractual Deliverables; and

- Service Level Requirements (SLR) and Priority Matrix.

The SDM document must be reviewed and modified as necessary, approved by SSC and signed-off on a quarterly basis.

2.1.9.2 General Management Documentation (GMD)

The GMD describes the Contractor's organization relative to the Service Desk Services contract, the roles and responsibilities of the key personnel, the service provider's management escalation process, management processes, communication plan and interaction or interdependencies between the service provider's managed functions and other Domains and SSC.

The service provider must update the GMD quarterly and provide it to the appropriate designated SSC Manager for approval and distribution to SSC Management.

The GMD document must be reviewed and modified as necessary, approved by SSC and signed-off on a quarterly basis.

3.0 Service Management Services Requirements

The Contractor is responsible for providing the Service Management Services defined in this document across the Service Desk Service Lines described in **Schedule A 1 – Service Desk Services**.

In all tables in this section, an "X" is placed in the column named "Contractor" to indicate that the Contractor must perform the task. Where an "X" is placed in the column "SSC" the contractor is not required to perform the task. Any approval and/or review will be the responsibility of SSC.

3.1 Service Descriptions and Roles and Responsibilities

3.1.1 General Responsibilities

The following table identifies General Roles and Responsibilities associated with the Service Management Services that the Parties must perform.

Table 29: General Services Roles and Responsibilities

Identifier	General Services Roles and Responsibilities	Contractor	SSC
1.01	Provide Service Management Services and develop processes (such as ITIL Service Management processes) that support SSC business and service requirements.		X
1.02	Approve Service Management Services and associated processes that support SSC business needs and service requirements.		X
1.03	Comply with GC and SSC guiding principles, policies and standards, as well as regulatory requirements applicable to SSC for information, information technology and systems, personnel, physical and technical security.	X	
1.04	Develop and maintain standards, processes and procedures that will be used in the delivery of all Service Desk Services (per Section 3.0 of this document) and collected in the Service Delivery Manual, which will include clearly delineated processes, roles and responsibilities and measurements that SSC and the Contractor will use to deliver SSC services.	X	
1.05	Approve the Service Delivery Manual, including all component standards, processes and procedures that will be used in the delivery of Service Desk Services.		X
1.06	Conform to changes in laws, regulations and policies. Major Service Changes must be proposed on a project-by-project basis of effort to alter the environment to conform to new requirements.	X	
1.07	Report performance against SLRs.	X	

Identifier	General Services Roles and Responsibilities	Contractor	SSC
1.08	Provide timely creation, updating, maintenance and provisioning of all appropriate plans, time and cost estimates, technical specifications, management documentation and management reporting in a format that is acceptable to SSC for all major Service Desk Service changes.	X	
1.09	Adhere to ITIL best practices and SSC-approved Key Performance Indicators (KPIs), per **Schedule A 4. Governance and Relationship Management Services**.	X	
1.10	Approve the use of ITIL best practices and KPIs.		X

3.1.2 Service Desk Service IT Life Cycle and Operations

3.1.2.1 Planning and Analysis Services

Planning and Analysis Services are activities associated with researching new technical trends, products and services such as Service Desk equipment components and systems software that offer opportunities to improve the efficiency and effectiveness of the Service Desk Services. Planning and Analysis Services must also support competitive business advantage and mitigate risks by reducing defects and improving the Quality of Services. The following table identifies the Planning and Analysis roles and responsibilities that the Parties must perform.

Table 30: Planning and Analysis Services Roles and Responsibilities

Identifier	Planning and Analysis Services Roles and Responsibilities	Contractor	SSC
2.01	Provide corporate business goals and objectives, information system roadmaps, the IT governance model, and IT risk issues and opportunities.		X
2.02	Define services, processes and standards for Planning and Analysis Services.	X	
2.03	Review and approve services, processes and standards for Planning and Analysis Services.		X
2.04	Define SSC enterprise-level requirements: e.g., business, technology strategy, functional, availability, capacity, performance and IM-IT Service continuity.		X
2.05	Perform Service Planning and Analysis based on SSC requirements: e.g., availability, capacity, performance, and Disaster Recovery (DR) Services support in addition to DR for vendor-owned services).	X	
2.06	Provide recommendations for new or changes to in-scope applications, processes and services based on Planning and Analysis Services results.	X	
2.07	Approve recommendations for new or changes to applications, processes and services.		X
2.08	Provide management reports required for Planning and Analysis Services: e.g., utilization and capacity trend reports, rollout plans.	X	
2.09	Define Data Backup and Retention policies for Service Desk Services.		X
2.10	In the context of Service Desk Services, continuously monitor technical trends through independent research; and document and report on products, processes and services with potential use to align with SSC business and technology strategy.	X	
2.11	Perform feasibility studies if needed for the implementation of new technologies that best meet SSC business needs and meet cost, performance and quality objectives.	X	
2.12	Define enterprise-level deployment management policies, procedures and requirements: e.g., feasibility analysis, cost-benefit analysis, scheduling, costing, resource planning, communication planning, procurement, risk management and quality management.		X
2.13	Perform management function for Contractor-managed Planning and Analysis activities.	X	

Identifier	Planning and Analysis Services Roles and Responsibilities	Contractor	SSC
2.14	Provide management oversight to the business and to the liaison function to customers.		X
2.15	Conduct regular planning for technology refreshes and upgrades.		X
2.16	Contribute as required to planning for technology refreshes and upgrades.	X	
2.17	Conduct quarterly technical reviews and provide recommendations for Service Desk Services improvements that align to SSC business goals.	X	

3.1.2.2 Requirements Definition Services

Requirements Definition Services are the activities associated with the assessment and definition of requirements related to the technical design of Service Line Services and Service Management Service activities. These requirements drive the technical design for the IM-IT environment. The following table identifies the Requirements Definition roles and responsibilities that the Parties must perform.

Table 31: Requirements Definition Services Roles and Responsibilities

Identifier	Requirements Definition Services Roles and Responsibilities	Contractor	SSC
3.01	Define and document requirements for the technical design of the environment.		X
3.02	Participate in defining requirements for the technical design of the environment.	X	
3.03	Document requirements to deliver Services in an SSC-agreed format.	X	
3.04	Ensure defined requirements respond to and comply with SSC policies, procedures and applicable government regulations outlined in **Schedule A 10 – Policies and Procedures**.	X	
3.05	Approve all requirements.		X
3.06	Define Acceptance Test Criteria.	X	
3.07	Review and approve all Acceptance Test Criteria.		X
3.08	Provide documented requirements and Acceptance Test Criteria per approved requirements by SSC.	X	

3.1.2.3 Design Specification Services

Design Specification Services are the activities associated with translating user and information system requirements into detailed technical specifications. The following table identifies the Design Specifications Services roles and responsibilities that the Parties must perform.

Table 32: Design Specifications Services Roles and Responsibilities

Identifier	Design Specification Services Roles and Responsibilities	Contractor	SSC
4.01	Define Design Specifications Services standards and requirements.		X
4.02	Develop, document and maintain technical design plans and IM-IT environment configuration based on SSC Design Specifications Services standards and requirements, including IT architecture, functional, performance, availability, maintainability and disaster recovery requirements.	X	
4.03	Determine and document required Service Line component upgrades, replacement and/or conversion specifications (e.g., Equipment, Software, etc.).	X	
4.04	Review and approve design plans through coordination with the appropriate SSC technology standards group(s) and design architects.		X
4.05	Provide written information in sufficient detail pertaining to Design Specifications to enable creation of the appropriate design documents.		X

Identifier	Design Specification Services Roles and Responsibilities	Contractor	SSC
4.06	Document and deliver Design Specifications.	X	
4.07	Review and approve Design Specifications.		X

3.1.2.4 Implementation and Migration Services

Implementation and Migration Services are the activities associated with the installation of new and/or upgraded Service Line components or Services into the Contractor's operational environment. The following table identifies the Implementation and Migration roles and responsibilities that the Parties must perform.

Table 33: Implementation and Migration Services Roles and Responsibilities

Identifier	Implementation and Migration Services Roles and Responsibilities	Contractor	SSC
5.01	Define Implementation and Migration requirements and policies.		X
5.02	Develop, document and maintain Implementation and Migration procedures that meet requirements and adhere to defined policies.	X	
5.03	Review and approve Implementation and Migration Services procedures.		X
5.04	Notify SSC of equipment migration and redeployment plans and schedules.	X	
5.05	Review all Implementation and Migration plans and schedules with SSC.	X	
5.06	Approve Implementation and Migration plans and schedules.		X
5.07	Coordinate infrastructure changes as required between SSC IM-IT staff and Contractor IM-IT staff.	X	
5.08	Install physical infrastructure as required (e.g., wiring, cable plant, cooling, etc.) in Contractor facilities.	X	
5.09	Coordinate Implementation and Migration support activities between SSC IM-IT staff and Contractor IM-IT staff.	X	
5.10	Install, integrate and/or migrate new and upgraded Service Line components or Services into Contractor's operational environment.	X	
5.11	Perform validation tests on all new and upgraded Service Line components or Services.	X	
5.12	Approve successful implementation of new and upgraded Service Line components or Services.		X
5.13	Update all documentation to new and upgraded Service Line components or Services.	X	

3.1.2.5 Training and Knowledge Transfer Services

Training and Knowledge Transfer Services includes maintaining an internal Training Program to deliver education and instruction to the Contractor's staff. The Contractor must participate in initial and ongoing training as required and approved by SSC to provide a learning opportunity to Contractor's staff about the SSC IM-IT environment as related to Service Desk Services. The following table identifies the Training and Knowledge Transfer Services roles and responsibilities that the Parties must perform.

Table 34: Training and Knowledge Transfer Services Roles and Responsibilities

Identifier	Training and Knowledge Transfer Services Roles and Responsibilities	Contractor	SSC
6.01	Define Training and Knowledge Transfer requirements and policies.		X
6.02	Develop, document and maintain Training and Knowledge Transfer procedures that meet requirements and adhere to defined policies.	X	
6.03	Review and approve Training and Knowledge Transfer procedures.		X
6.04	Develop, implement and maintain an accessible knowledge database/portal.		X

Identifier	Training and Knowledge Transfer Services Roles and Responsibilities	Contractor	SSC
6.05	Develop and implement Knowledge Transfer procedures to ensure that more than one individual understands key components of the business and technical environment.	X	
6.06	Participate in SSC-delivered instruction on the business and technical environment.	X	
6.07	Develop, document and deliver internal Contractor training requirements that support the ongoing provision of SSC Services, including refresher courses as needed and instruction on new functionality.	X	
6.08	Take training classes as needed to remain current with systems, software, features and functions for which Service Desk Services support is provided, in order to improve Service performance (e.g., First-Contact Resolution).	X	
6.09	Provide training when substantive (as defined between SSC and Contractor) technological Changes (e.g., new systems or functionality) are introduced into the SSC environment, in order to fully exploit all relevant functional features.		X
6.10	Provide ongoing training materials for Service Desk personnel on SSC business and technical environments.	X	

3.1.2.6 Documentation Services

Documentation Services are the activities associated with developing, revising, maintaining, reproducing and distributing Service Line Service information in hard copy and electronic form. The following table identifies the Documentation roles and responsibilities that the Parties must perform.

Table 35: Documentation Services Roles and Responsibilities

Identifier	Documentation Services Roles and Responsibilities	Contractor	SSC
7.01	Recommend Documentation requirements and formats.	X	
7.02	Define Documentation requirements, formats and policies.		X
7.03	Provide the Contractor information necessary to develop training documentation, policy guides, reference manuals, procedures and support scripts necessary for Service Desk staff and technicians to function appropriately.		X
7.04	Develop, document and maintain Documentation procedures that meet requirements and adhere to defined policies.	X	
7.05	Review and approve Documentation procedures.		X
7.06	Provide output in agreed formats (i.e., MS Word, PDF or mutually accessible Knowledge Base) for support of activities throughout the life cycle of Services as specified for each Service Line.	X	
7.07	Maintain and update documentation for system specifications and configurations (e.g., interconnection topology, configurations, and network diagrams). Create documentation when new capabilities or changes are introduced.	X	
7.08	Provide SSC-specific operating requirements.		X
7.09	Document Standard Operating Procedures (e.g., boot, failover, batch processing, backup).	X	
7.10	Review and approve the Standard Operating Procedures.		X
7.11	Document job production and maintenance schedules.	X	
7.12	Review and approve job production and maintenance schedules and Documentation.		X
7.13	Develop the list of standard Service Line Services and products, including standard and available non-standard Equipment and Software configurations, and a list of services with standard cycle times.		X
7.14	Support development and update of list(s) in 7.13 and maintain lists.	X	

3.1.3 Service Delivery

3.1.3.1 Capacity Management Services

In the context of tools, systems and resources that the Contractor provides to support the Service Line Services, Capacity Management Services are the activities associated with ensuring that the capacity of the Service Line Services matches the evolving demands of SSC's business in the most cost-effective and timely manner. The process encompasses the following:

- Monitoring performance and throughput of Service Line Services and supporting IT components;
- Understanding current demands and forecasting for future requirements;
- Developing capacity plans to meet demand and SLRs;
- Conducting regular risk assessments of capacity recommendations;
- Developing and implementing a capacity plan, including the financial impact of the Service Lines; and
- Undertaking tuning activities.

The following table identifies the Capacity Management roles and responsibilities that the Parties must perform.

Table 36: Capacity Management Services Roles and Responsibilities

Identifier	Capacity Management Services Roles and Responsibilities	Contractor	SSC
8.01	Define Capacity Management requirements (SLRs) and policies.		X
8.02	Develop, document and maintain Capacity Management processes and procedures that meet requirements and adhere to defined policies.	X	
8.03	Review and approve Capacity Management processes and procedures.		X
8.04	Establish a comprehensive Capacity Management planning process.	X	
8.05	Review and approve Capacity Management planning process.		X
8.06	Define, develop and implement tools that allow for the effective capacity monitoring/trending of IT infrastructure, applications and IT components.	X	
8.07	Identify future business requirements that will alter capacity requirements.		X
8.08	Develop a quarterly Capacity Plan.	X	
8.09	Develop and implement capacity models to validate the Capacity Plan.	X	
8.10	Participate in capacity planning activities where applicable.		X
8.11	Assess capacity impacts when adding, removing or modifying applications and infrastructure components.	X	
8.12	Continually monitor IT resource usage to enable proactive identification of capacity and performance issues.	X	
8.13	Capture trending information and forecast future SSC capacity requirements based on SSC-defined thresholds.	X	
8.14	Assess Incidents/Problems related to capacity and provide recommendations for resolution.	X	
8.15	Recommend changes to capacity to improve service performance.	X	
8.16	Assess impact/risk and cost of capacity changes.	X	
8.17	Approve capacity-related recommendations.		X
8.18	Maintain capacity levels to optimize use of existing IT resources and minimize SSC costs to deliver Services respecting SLRs.	X	
8.19	Ensure adequate capacity exists within the Service Line Service environment to meet SLR requirements taking into account daily, weekly and seasonal variations in capacity demands.	X	
8.20	Validate Asset utilization and capital efficiency.		X

3.1.3.2 Performance Management Services

Performance Management Services are the activities associated with managing and tuning Service Line components for optimal performance. The process encompasses the following:

- Monitoring of performance and throughput of Service Line Services and supporting IT components;
- Assessing the results of the reports;
- Conducting trending analysis;
- Providing recommendations to tuning; and
- Performing tuning activities.

The following table identifies the Performance Management Services roles and responsibilities that the Parties must perform.

Table 37: Performance Management Services Roles and Responsibilities

Identifier	Performance Management Services Roles and Responsibilities	Contractor	SSC
9.01	Define Performance Management requirements and policies.		X
9.02	Develop, document and maintain Performance Management procedures that meet requirements and adhere to defined policies.	X	
9.03	Review and approve Performance Management procedures.		X
9.04	Perform Service Line component tuning to maintain optimum performance in accordance with Change Management procedures.	X	
9.05	Manage Contractor resources supporting the Service Line (e.g., computing devices, internet connections and telephones) to meet defined Availability and performance SLRs.	X	
9.06	Provide regular monitoring and reporting of resources supporting the Service Line performance, utilization and efficiency.	X	
9.07	Proactively evaluate, identify and recommend configurations or changes to configurations that will enhance performance.	X	
9.08	Conduct trending analysis to recommend changes to improve the performance.	X	
9.09	Develop and deliver improvement plans as required to meet SLRs.	X	
9.10	Review and approve improvement plans.		X
9.11	Implement improvement plans.	X	
9.12	Coordinate with Third Parties (e.g., hardware, software and equipment vendors).		X
9.13	Provide technical advice and support to the application maintenance and development staff as required.	X	

3.1.3.3 Service Level Monitoring and Reporting Services Roles and Responsibilities

Service Level Monitoring and Reporting Services are the activities associated with the monitoring and reporting against SLRs. In addition, the Contractor shall report system management information (e.g., performance metrics and system accounting information) to the designated SSC representatives in a format agreed to by SSC. The following table identifies the Service Level Monitoring and Reporting roles and responsibilities that the Contractor must perform.

Table 38: Service Level Monitoring and Reporting Services Roles and Responsibilities

Identifier	Service Level Monitoring Roles and Responsibilities	Contractor	SSC
10.01	Define SLRs.		X
10.02	Define Service Level Monitoring and Reporting requirements and policies.		X
10.03	Develop, document and maintain Service Level Monitoring and Reporting procedures that meet requirements and adhere to defined policies.	X	
10.04	Review and approve Service Level Monitoring and Reporting procedures.		X
10.05	Report on SLR performance and improvement results.	X	
10.06	Coordinate SLR monitoring and reporting with designated SSC representative and Third Parties.	X	
10.07	Measure, analyze and provide management reports on performance relative to SLRs.	X	

Identifier	Service Level Monitoring Roles and Responsibilities	Contractor	SSC
10.08	Conduct SLR and Monitoring Improvement Meetings to review SLRs and recommendations for improvements.	X	
10.09	Review and approve SLR and Monitoring improvement plans.		X
10.10	Implement SLR and Monitoring improvement plans.	X	
10.11	Review and approve SLR metrics and performance reports.		X
10.12	Provide SSC access to performance and SLR reporting and monitoring system and data.	X	

3.1.3.4 Security Services

In the context of tools, systems and resources that the vendor provides to support the Service Line Services, Security Services are the activities associated with maintaining physical and logical security of all Contractor components (Equipment and Software) supporting the Service Line, including data, virus protection, access protection and other Security Services in compliance with GC and SSC Security requirements and all applicable regulatory requirements. The following table identifies Security roles and responsibilities that the Parties must perform.

Table 39: Security Services Roles and Responsibilities

Identifier	Security Services Roles and Responsibilities	Contractor	SSC
11.01	Define Security requirements, standards, processes, procedures and policies.		X
11.02	Develop, document and maintain Security requirements, standards, processes, procedures and policies, including regulatory requirements.	X	
11.03	Review and approve Security requirements, standards, processes, procedures and policies, including regulatory requirements.		X
11.04	Remain up-to-date on current Security trends, threats, common exploits and security policies and procedures and best practices.	X	
11.05	Ensure that all Contractor employees have appropriate Security clearances.	X	
11.06	As required, provide an Information Security Advisor that will be the direct liaison with SSC for Security requirements.	X	
11.07	Conduct risk assessments to identify control or Security gaps.	X	
11.08	Implement physical and logical Security Plans consistent with SSC Security policies and industry standards in Contractor facilities (e.g., Canadian Industrial Security Division standards).	X	
11.09	Report and Resolve Security Incidents to SSC per SSC policies, outlined in **Schedule A 10 — Policies and Procedures**.	X	
11.10	Review and install all Security patches relevant to the IT environment as per SSC Security requirements.	X	
11.11	Participate in and support SSC Security Awareness Programs.	X	
11.12	Perform periodic Security audits.		X
11.13	Support SSC and SSC-approved Third Party Security Audits.	X	

3.1.3.5 Service Continuity and Disaster Recovery Services

The Contractor must demonstrate that it will consistently meet or exceed SSC Service Continuity and Disaster Recovery Services requirements for facilities and services provided by the Contractor. The following table identifies Service Continuity and Disaster Recovery Services roles and responsibilities that the Contractor must perform.

Table 40: Service Continuity and Disaster Recovery Services Roles and Responsibilities

Identifier	Service Continuity and Disaster Recovery Roles and Responsibilities	Contractor	SSC
12.01	Define SSC-related Disaster Recovery Service requirements.		X
12.02	Recommend SSC-related best practices for Disaster Recovery Service strategies, processes and procedures.	X	

Identifier	Service Continuity and Disaster Recovery Roles and Responsibilities	Contractor	SSC
12.03	Document SSC-related Disaster Recovery Service process and procedures that adhere to SSC requirements.	X	
12.04	Review and approve SSC-related Disaster Recovery Service procedures.		X
12.05	As needed, assist SSC in other IT continuity and emergency management activities.	X	
12.06	Develop and maintain a detailed plan to meet Disaster Recovery requirements. The Plan shall include specific plans for data, backups, storage management and contingency operations within established recovery requirement timeframes for the in-scope Service Line Services after a disaster affects use of the Services.	X	
12.07	Establish processes to ensure Disaster Recovery Plans are kept up-to-date and reflect Changes in the SSC environment.	X	
12.08	Test the Disaster Recovery Plan on an annual basis and report results to SSC.	X	

4.0 Service Level Requirements

All SLRs related to the delivery and service management of Service Desk Services are detailed in **Schedule B 2 – Service Level Requirements**.

The Contractor must consistently meet or exceed the defined SLRs for the Service Line Services (and other Services where applicable). Any Services developed by the Contractor pursuant to this Contract must incorporate methods permitting measurement of performance-related SLRs. The Contractor must comply with all SLRs set forth in the Statement of Work.

Defined SLRs represent minimum Service levels required, which must be consistently met or exceeded.

Schedule A 3 - Transition Service

Shared Services Canada (SSC)

Schedule A 3 - Transition Service

Table of Contents

List of Tables

Schedule A 3 - Transition Service

1.0 Transition Service Overview and Service Objectives

1.1 Transition Service Overview

This Schedule sets forth the services, roles and responsibilities of the Parties under the Contract in order for Service Desk Services described in **Schedule A 1 – Service Desk Services,** to be transitioned to the Contractor. Transition includes initial planning and development of a Transition Project Plan, including planning activities performed with the current SSC contractor (Service Desk Service provider) where applicable. It also includes the activities necessary to assume full responsibility for all in-scope services and supporting Service Management activities described in **Schedule A 2 – Service Management Services**.

1.2 Transition Service Objectives

The Contractor must achieve the following key high-level Transition objectives:

a. Provide a focused plan that will accelerate and expedite Transition of Services.

b. Perform all Knowledge Transfer activities necessary to assume the Services under this Contract.

c. Work with SSC and its current contractor (the provider(s) of existing Service Desk Services) to transfer, and/or assign rights under any existing equipment or software or other contractual agreements (which may be applicable to SSC) necessary to assume the Services under this Contract, as applicable.

d. Assume responsibility for the performance of all Systems, Software and Hardware in accordance with the Statements of Work and Service Level Requirements (SLRs) under this Contract.

e. Integrate all operational systems into the Contactor's operations including, but not limited to, ticketing systems, reporting systems, tracking and management systems and phone systems necessary to perform the Services under this Contract.

f. Put in place infrastructure and processes necessary to perform the Services under this Contract.

g. Hire and train necessary Contractor Personnel to perform the Services under this Contract.

h. Mitigate any and all risks or possibility of outage or significant degradation of any System or processes that could be caused by Transition activities.

2.0 Service Environment

Schedule A 1 – Service Desk Services and **Schedule A 2 – Service Management Services** describe the service environment and in-scope services to be supported and/or for which the Contractor must comply. The following further describes the service environment to be supported in relation to this Schedule.

2.1 Scope of the Transition

The scope of the Transition includes all activities necessary to begin performance of the activities defined in the Contract Statement of Work (SOW), specifically:

1. Schedule A 1 – Service Desk Service;
2. Schedule A 2 – Service Management Service;
3. Schedule A 3 – Transition Service; and
4. Schedule A 4 – Governance and Relationship Management Service.

3.0 Transition Service Requirements

3.1 Service Descriptions and Roles and Responsibilities

In all tables included in this section, an "X" is placed in the "Contractor" column to indicate that the Contractor must perform the task. Where an "X" is placed in the "SSC" column the Contractor is not required to perform the task. Any approval and/or review will be the responsibility of SSC.

3.1.1 General Role and Responsibilities

The following table identifies the General Roles and Responsibilities that the Parties must perform.

Table 41: General Roles and Responsibilities

Identifier	General Roles and Responsibilities	Contractor	SSC
1.01	Understand and comply with SSC policies and procedures throughout Transition.	X	
1.02	Recommend an overall Transition Methodology and develop Project Plan.	X	
1.03	Provide input to the Transition Project Plan and coordinate input of Third-Party suppliers, such as the current service provider (contractor), or other Third-Parties as identified by SSC.	X	
1.04	Approve the Transition Methodology and Project Plan.		X
1.05	Provide overall Transition Project Manager and Transition support personnel.	X	
1.06	Provide SSC Transition Project Manager with overall responsibility for SSC Transition tasks.		X
1.07	Provide access to Information Technology systems and tools necessary to support Transition, including access requests, SSC equipment and Software licenses, and access to required Subject Matter Experts.		X
1.08	Provide weekly status reports on overall adherence to the Transition Project Plan, including completion status, estimated completion dates (ECD), risks and risk mitigation plans, rescheduled requirements, issues, and help needed.	X	
1.09	Show evidence of adherence to plans and milestones, including documentation showing successful completion of knowledge transfer activities, agreement from current contractor(s) that the Contractor is able to perform responsibilities of the SOW, and demonstration of other tasks completion as may be required by the Transition Project Plan.	X	
1.10	Close actions identified during transition and Governance meetings in a timely manner, as agreed on during the meetings.	X	
1.11	Maintain general management of the Transition process.	X	

3.1.2 Transition Project Planning

The Contractor must provide a Preliminary Transition Project Plan (see requirements in Appendix A – Preliminary Transition Plan to this schedule) with their response to the Request for Proposal. After contract award, the Contractor will present to SSC their detailed Transition Project Plan and schedule for review and approval within 10 Federal Government Working Days (FGWD) of the scheduled kick-off meeting between SSC and the Contractor. The Transition Project Plan, developed with input from all key stakeholders, will include a detailed schedule, with estimated completion dates and resources identified for all tasks. As part of the Transition Project Plan, the Contractor must provide a documented Project Status process which includes, at a minimum:

a. Procedures for updating the Transition Project Plan;

b. Regularly scheduled meetings;

c. Escalation procedures;

d. Risk management procedures;

e. Criteria for determining successful completion of milestones defined in the Transition Project Plan; and;

f. Weekly reporting of overall adherence to the Transition Project Plan.

The following table identifies the Transition Project Planning Roles and Responsibilities that the Parties must perform.

Table 42: Transition Project Planning Roles and Responsibilities

Identifier	Transition Project Planning Roles and Responsibilities	Contractor	SSC
2.01	Propose Transition Project Plan and define Project Charter to support integrated Transition planning and execution.	X	
2.02	Approve Transition Project Plan and Project Charter.		X
2.03	Propose Transition Project Staffing Plan and organization.	X	
2.04	Work jointly with both SSC and current contractors (as defined in 3.1.2, above) to obtain input for Transition Project Plan and submit it for approval.	X	
2.05	Approve Contractor's Transition Project Staffing Plan and organization.		X
2.06	Provide experienced personnel for Transition, including a lead Transition Project Manager.	X	
2.07	Provide experienced SSC personnel for Transition, including a lead Transition Project Director.		X
2.08	Propose meeting schedule and appropriate project management processes and procedures.	X	
2.09	Approve meeting schedule and project management processes and procedures.		X
2.10	Identify high-risk Transition areas and impacts, develop mitigation strategies, recommend Mitigation Plans and report results to SSC using a risk log.	X	
2.11	Review the risk log and mitigation plans, and determine with the Contractor's assistance the appropriate mitigation strategies and courses of action to take.		X
2.12	Develop, update, maintain, and revise a detailed Transition Project Plan(s) that includes approach, activities, milestones, schedule, and risk identification and mitigation strategies/plans.	X	
2.13	Work with any Third-Party representatives designated by SSC (e.g., current service contractor(s)), as part of Transition oversight.	X	
2.14	Approve Transition Project Plan(s), schedules, and related documentation, including all plan revisions.		X
2.15	Provide status reports and risk mitigation plans.	X	
2.16	Approve risk mitigation plans.		X

3.1.3 Tools and Software Transition

Tools and Software Transition includes all activities to transition access to the Contractor of all tools and software necessary for the Contractor to provide all services within the scope of this Contract and specifically detailed in **Schedule B 3 – Financial Responsibilities Matrix**. Upon completion of Transition, the Contractor must provide all Services in this Statement of Work (SOW) using a combination of tools that may include those in that Schedule. Completion and Acceptance must be confirmed by SSC and the Contractor certifying that the Contractor is prepared to begin providing the Services defined in the SOW.

The following table identifies the Tools and Software Transition Roles and Responsibilities that the Parties must perform.

Table 43: Tools and Software Transition Roles and Responsibilities

Identifier	Tools and Software Transition Roles and Responsibilities	Contractor	SSC
3.01	Propose Knowledge Transfer Plan to support transition of access to the Contractor of all tools and software.	X	
3.02	Approve the Knowledge Transfer Plan.		X
3.03	Perform Knowledge Transition with SSC, suppliers and/or current contractors (i.e., Third Parties with whom SSC has a business relationship in the provision of in-scope services).	X	
3.04	Coordinate implementation of new tools or customization of existing tools to enable the support environment.	X	
3.05	Document knowledge transfer activity and system administration tasks in SSC Knowledge Management System.	X	
3.06	Define and recommend cutover readiness criteria and Transition Plan milestones.	X	
3.07	Approve recommended cutover readiness criteria.		X
3.08	Execute on readiness criteria being met.	X	
3.09	Review and approve Contractor's completion of readiness criteria.		X
3.10	Work with current contractor(s) to support the Transition Project Plan milestones.	X	

3.1.4 Service Transition Approach per Statement of Work

A comprehensive list of governance processes and procedures will be jointly defined by SSC and the Contractor as part of Transition Services planning. These processes and procedures must be identified within sixty (60) FWGDs of Contract Award and will include, but not be limited to:

- Change Management;
- Customer Satisfaction Management;
- Quality Assurance;
- Dispute Resolution;
- Integration Management;
- Performance Reporting, such as reporting on Service Level Requirements (SLRs), project status, and outstanding Service Request status;
- Human Resource Management;
- Service Level Management;
- Strategy and Planning; and
- Financial Management, including Additional Resource Charges / Reduced Resource Credits (ARC/RCC) Management.

The following table identifies the Service Transition Approach Roles and Responsibilities that the Parties must perform.

Table 44: Service Transition Approach Roles and Responsibilities

Identifier	Service Transition Approach Roles and Responsibilities	Contractor	SSC
Transition Kickoff and Management			
4.01	Establish framework for Service Delivery (processes and procedures), evaluate existing processes, and conduct gap analysis.	X	
4.02	Provide standardized processes and/or templates using automated tools whenever possible, which at a minimum, must include the following: • Risk Log; • Issue Log; • Integrated Milestone Schedule; • Status Report/Performance Report; • Change Control processes/templates;	X	

Identifier	Service Transition Approach Roles and Responsibilities	Contractor	SSC
	• Communication processes; • Change Management Plan (Training, etc.); and • IT Knowledge Management/document repository tools.		
4.03	Submit processes and templates for approval.	X	
4.04	Approve processes and templates.		X
4.05	Develop a comprehensive Human Resources Sourcing and Retention Strategy, including, but not limited to, acquiring, training and retaining certified bilingual staff with the skills necessary to provide high-quality Service Desk Services.	X	
4.06	Review and provide feedback on the Human Resources Sourcing and Retention Strategy (which will be the subject of ongoing governance under Resource Management, delineated in **Schedule A 4 – Governance and Relationship Management Service**).		X
4.07	Develop comprehensive Program for Monitoring Customer (end-user/partner service desk agent) Satisfaction (including but not limited to, baseline measurement, survey templates, scope, frequency and scoring grid). The Program for Measurement of Customer Satisfaction must address both the Customer Satisfaction (CSAT) Service Level Category and the continuous improvement requirement established in Section 11.0 of **Schedule B 2 – Service Level Requirements.**	X	
4.08	Approve comprehensive Program for Monitoring Customer Satisfaction.		X
4.09	Develop comprehensive Quality Assurance Program (including, but not limited to, baseline measurement, scoring templates, scope and frequency of samples). The Quality Assurance Program must address both the Quality Assurance (QA) Service Level Category and the continuous improvement requirement established in Section 11.0 of **Schedule B 2 – Service Level Requirements.**	X	
4.11	Approve comprehensive Quality Assurance Program.		X
4.12	Create Governance and Partner / Non-Partner Service Desk Agent experience measurement processes.	X	
4.13	Document existing baseline including: high-level process maps; standard operating procedures; customer service levels; client satisfaction levels and operational activities for use in Transition planning, readiness, cutover and stabilization activities.	X	
4.14	Create baselines and forecasts required with respect to number of contacts/ticket volumes, resolution rates, and number of users.	X	
4.15	Establish resolution expectations for those reported incidents / service requests handled by the Enterprise Service Desk (i.e. what issues should be resolved by ESD Service Desk Agents and what issues should be assigned to Service Line Resolver Groups). See potential contacts listed in **Schedule A 13 – Types of Contacts Handled**.		X
4.16	Establish resolution expectations for those reported incidents / service requests handled by the End User Service Desk (i.e. what issues should be resolved by EUSD Service Desk Agents and what issues should be escalated to the ESD). See potential contacts listed in **Schedule A 13 – Types of Contacts Handled**.		X
4.17	Agreement on Standard Format for Root Cause Analysis Reports.	X	X
4.18	Agreement on Standard Format for Corrective Action Plans.	X	X

3.1.5 Transition and Migration

Transition and Migration includes the activities associated with the preparation of the current SSC environment for transition to the Contractor. The following table identifies the Transition and Migration Services Roles and Responsibilities that the Parties must perform.

Table 45: Transition and Migration Roles and Responsibilities

Identifier	Transition and Migration Roles and Responsibilities	Contractor	SSC
Transition Kickoff and Management			
5.01	Execute Transition Project Plan(s).	X	
5.02	Provide Program Office Transition Status Report(s).	X	
5.03	Manage, update, and maintain a detailed Transition schedule(s) that includes activities, deliverables, milestones, and dependencies/linkages to current contractor schedules.	X	
5.04	Identify, develop and report on Transition schedule critical-path activities on a weekly basis and escalate issues as required to SSC.	X	
5.05	Conduct readiness planning activities per the Approved Transition Project Plan.	X	
5.06	Participate in readiness planning per the approved Transition Project Plan.		X
5.07	Conduct Service cutover planning activities per the approved Transition Project Plan(s) resulting in a proposed Cutover Plan.	X	
5.08	Participate in cutover planning per the approved Transition Project Plan(s), and approve the Cutover Plan.		X
Readiness Assessment			
5.09	Develop a thorough Implementation Readiness Assessment Plan, readiness assessment schedule, rollback strategy, assessment scorecards, and defined critical readiness criteria to drive Go/No-Go decisions related to overall readiness/preparedness for going live with in-scope services.	X	
5.10	Approve Readiness Assessment Plan.		X
5.11	Conduct implementation readiness assessments and prepare report findings and recommendations on a weekly basis prior to cutover, and identify any items or situations that will impede successful cutover.	X	
5.12	Perform and complete remediation actions based on readiness assessments, and report status to SSC.	X	
5.13	Verify that all work, testing, evaluation, assessments, and corrective remediation activities are performed and successfully completed to ensure 100% implementation readiness for all implementation criteria, prior to going live.	X	
5.14	Work with SSC to develop the necessary stakeholder communications and engagement plan, activities and collateral during pre-implementation.	X	
5.15	Review and deploy stakeholder communications and engagement activities during pre-implementation.		X
5.16	Support SSC to collect, analyze and report stakeholder feedback issues, comments and/or requests.	X	
5.17	Provide recommendations on the best course(s) of action to address/resolve stakeholder issues.	X	
5.18	Review stakeholder reports and authorize acceptable resolution actions.		X
Implementation			
5.19	Develop a detailed Implementation Plan, including a pre-implementation checklist, cut-over plan, and post-implementation evaluation criteria.	X	
5.20	Review and approve the Implementation Plan.		X
5.21	Make Go/No-Go recommendations and prepare a Go/No-Go Decision Document for approval.	X	
5.22	Approve Go/No-Go Decision Document.		X
5.23	Work with SSC to develop the necessary stakeholder communications and engagement plan, activities and collateral during implementation.	X	
5.24	Review and deploy stakeholder communications and engagement activities during cutover.		X
5.25	Collect, analyze and report stakeholder feedback issues, comments and or requests.		X

Identifier	Transition and Migration Roles and Responsibilities	Contractor	SSC
5.26	Review stakeholder reports and propose appropriate corrective action plan	X	
5.27	Review corrective action plan and authorize acceptable resolution actions.		X
5.28	Manage implementation and cutover in accordance with Implementation Plan ensuring no disruption to SSC service delivery.	X	
5.29	Conduct post-cutover inspection and submit completed post-cutover checklist within 24 hours following cutover.	X	
5.30	Ensure 100% completion of post-cutover activities per Cutover Plan.	X	

3.1.6 Transition Integration, Testing and Stabilization

Transition Integration, Testing and Stabilization includes the activities associated with a seamless Transition. The following tables identify Transition Integration, Testing and Stabilization Roles and Responsibilities that the Parties must perform.

Table 46: Transition Integration and Testing Roles and Responsibilities

Identifier	Transition Integration and Testing Roles and Responsibilities	Contractor	SSC
6.01	Provide proposed Integration and Testing Plan.	X	
6.02	Review and approve Integration and Testing Plan.		X
6.03	Recommend integration and testing requirements.	X	
6.04	Approve integration and testing requirements.		X
6.05	Develop, document and maintain Integration and Testing Plan that meets requirements and adheres to defined policies.	X	
6.06	Manage integration test environment.		X
6.07	Maintain Software release matrices across development, quality assurance, and production environments and networks.		X
6.08	Conduct integration and security testing for all data, infrastructure and networks based on requirements defined in the Integration and Testing Plan and SSC policies and procedures.	X	
6.09	Evaluate all services to be transitioned for compliance with SSC security rules, regulations and procedures.	X	
6.10	Assess and communicate the overall impact and potential risk prior to implementing changes.	X	
6.11	Define User Acceptance Test (UAT) requirements.		X
6.12	Develop UAT Plan per requirements.	X	
6.13	Review and approve UAT Plan.		X
6.14	Conduct UAT and document results per requirements.	X	
6.15	Share UAT test results with SSC.	X	
6.16	Review UAT results.		X
6.17	Propose changes to infrastructure, software or services based on testing results.	X	
6.18	Approve changes to infrastructure, software or services.		X
6.19	Approve Service Commencement (based on Go/No-Go Decision Document).		X
6.20	Stage new and upgraded infrastructure, software or services to smoothly transition into existing environment based on defined requirements.	X	

Table 47: Program Stabilization and Post-Transition

Identifier	Program Stabilization and Post-Transition Roles and Responsibilities	Contractor	SSC
Program Stabilization			

Identifier	Program Stabilization and Post-Transition Roles and Responsibilities	Contractor	SSC
7.01	Resolve any stabilization/post-cutover issues identified by SSC as highest-priority within 24 hours of cutover.	X	
7.02	Following cutover, conduct a stabilization assessment in accordance with the Transition Project Plan schedule, including recommendations for stabilization and improvement.	X	
7.03	Following cutover, complete all stabilization activities in accordance with the Transition Project Plan schedule.	X	
7.04	Work with SSC to develop the necessary stakeholder communications and engagement plan, activities and collateral during implementation.	X	
7.05	Review and deploy stakeholder communications and engagement activities during implementation.		X
7.06	Collect, analyze and report stakeholder feedback issues, comments and or requests.	X	
Post-Transition Review			
7.07	Conduct a post-Transition review within <TBD days> of cutover. Note: as per Section 3.1.2, <TBD days> will be confirmed in the Transition Plan.	X	
7.08	Document lessons learned from Transition.	X	
7.09	Incorporate lessons learned into subsequent Transition activities (e.g., future transitions, transition-out planning, etc.).	X	
7.10	Work with SSC to develop the necessary stakeholder communications and engagement plan, activities and collateral during post-Transition.	X	
7.11	Review and deploy stakeholder communications and engagement activities during post-Transition.		X
7.12	Collect, analyze and report stakeholder feedback issues, comments and requests.		X

3.2 Engagement of Key Contractor Personnel

See Section 2.0 of Schedule **A 4 – Governance and Relationship Management Services** for Contractor obligations with respect to the continued engagement of Key Contractor Personnel involved in Transition Services.

3.3 Exclusions

For greater certainty, any on-going service provided under this Contract are excluded from Transition Services.

4.0 Transition-Out

4.1 Transition-Out Overview

Transition-out activities must provide the materials and assistance to transition the Service Desk Services from the Contractor to a new service provider. The Contractor must work with SSC and another contractor(s) selected by SSC, if applicable, at the conclusion of the Contract, to transition the Service Desk Services, including training and knowledge transfer.

The Contractor must support an orderly and efficient transition of the services to the new service provider with minimal disruption of services to SSC, its service delivery and customers.

The Contractor must maintain sufficient qualified staff to meet all requirements of the Transition-Out Service.

4.2 Transition-Out Requirements

At the end of the contract, the Contractor must return to SSC all information, Service Desk Services data and equipment that are owned by SSC. The Contractor agrees that, in addition to other data not specifically identified here, SSC owns all information pertaining to SSC's processes, knowledge, FAQs, Incidents, and Service Requests that will be received and resolved by the Contractor over the term of the contract.

During transition-out, Contractor responsibilities include, but are not limited to, the delivery and/or support of the following activities:

a. Working closely with the new service provider on the planning, development and execution of the Transition-Out Project Plan.

b. Working with SSC and the new service provider to transfer and/or assign rights under any existing equipment, software or other contractual agreements necessary to assume the services under the future contract, as applicable.

c. Performing all knowledge transfer activities necessary and providing assistance as needed to enable a smooth transition, including the status of ongoing technical initiatives and the current status of service delivery.

d. Providing electronic copies of all materials developed to provide Service Desk services, including scripts, solutions, related materials, and the Service Delivery Manual. The electronic format for the materials will be specified by SSC to ensure compatibility with standard business software, such as Microsoft Office.

e. Providing Service Desk management and system data that enables the logs and summaries of the Service Desk Services provided under the contract to be accessed using standard business software, such as Microsoft Office.

f. Providing a complete extract of any supporting system data in a commercial off-the-shelf (COTS) file (e.g., in SQL or Excel format), as specified by SSC.

g. Returning to SSC all Government-furnished equipment / property that SSC provided to the Contractor.

At the end of the Contract, the Contractor must provide a debriefing to SSC to confirm that the Transition-Out is completed and transfer any remaining knowledge to SSC.

Appendix A — Preliminary Transition Plan

In their responses to the Request for Proposal, bidders will be required to provide a Preliminary Transition Plan. The Preliminary Transition Plan will be finalized within ten (10) FGWDs of kick-off meeting (see **Section 3.1.2 Transition Project Planning** of **Schedule A 3 – Transition Service**).

1.0 General Requirements

The efficient transition of the existing service desk support function (currently delivered by the Incumbent Contractor from the NCR) to fully managed Service Desk Services as described in **Schedule A 1 – Service Desk Services** (delivered by the Contractor from two facilities in the regions) must be completed in the allotted time frame with minimal disruption/degradation of service.

2.0 Expected Outcomes of the ESD and EUSD service transition

A successful transition will meet or exceed the following Outcomes:

- ✓ Will closely adhere to Deliverable Completion Deadlines and Milestone Delivery Dates;
- ✓ Will appear seamless to customers;
- ✓ Will have minimal impact on service level performance;
- ✓ Will result in an effective transfer of knowledge relating to tools, software, telephony platforms and service desk processes and procedures; and
- ✓ Will result in minimal duplication of costs to SSC through an efficient, synchronized ramp up of Contractor resources and ramp down of Incumbent Contractor resources.

3.0 Elements of Preliminary Transition Project Plan

The Preliminary Transition Plan should incorporate at a minimum, but should not be restricted to, the following elements:

- ✓ Contractor Key Personnel
- ✓ Project Status Process
- ✓ List of Deliverables
- ✓ List of Service Milestones/Delivery Dates/Milestone Payments

3.1 Contractor Key Personnel

The Preliminary Transition Project Plan should identify Key Contractor Resources to be engaged during the period of the transition. Dependencies and assumptions with respect to the involvement of Incumbent Contractor Personnel and SSC management personnel should be clearly articulated and quantified in the Preliminary Transition Project Plan.

3.2 Project Status Process

As part of the Preliminary Transition Project Plan, the Contractor must provide a documented Project Status Process which includes, at a minimum:

- ✓ Procedures for updating the Transition Project Plan;
- ✓ Regularly scheduled meetings;

- ✓ Escalation procedures;
- ✓ Risk management procedures;
- ✓ Criteria for determining successful completion of milestones defined in the Transition Project Plan; and;
- ✓ Weekly reporting of overall adherence to the Transition Project Plan.

3.3 List of Deliverables

As part of the Transition Services, without limiting any other Deliverables to be provided by Contractor, the Preliminary Transition Plan must include the following Deliverables:

Table 48: Preliminary Transition Plan

No	Deliverable Name	Completion Deadline	Acceptance Review Period	Acceptance Criteria
1.	Preliminary Transition Project Plan + Project Status Process	Bid Close	-	-
2.	Transition Project Plan	Within ten (10) FGWDs of kick-off	[SSC to provide]	[SSC to provide]
3.	Knowledge Transfer Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]
4.	Transition Project Charter	[Contractor to provide]	[SSC to provide]	[SSC to provide]
5.	Transition Project Staffing Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]
6.	Risk Mitigation Plan / Transition Risk Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]
7.	Human Resources Sourcing and Retention Strategy	[Contractor to provide]	[SSC to provide]	[SSC to provide]
8.	Stakeholder Engagement and Communications Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]
9.	Cutover Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]
10.	Readiness Assessment Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]
11.	Implementation Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]
12.	Integration and Testing Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]
13.	User Acceptance Test (UAT) Plan	[Contractor to provide]	[SSC to provide]	[SSC to provide]

3.4 List of Service Milestones/Delivery Dates/Milestone Payments

The Preliminary Transition Plan must include:

- ✓ Transition Service Milestone Descriptions
- ✓ Transition Milestone Delivery Dates for each Transition Service Milestone Description
- ✓ Transition Milestone Payment Amount for each Transition Service Milestone Description

If a Transition Milestone Delivery Date is not met, payment will not be made until that milestone is completed.

Schedule A 4 – Governance and Relationship Management Services

Shared Services Canada (SSC)

Schedule A 4 – Governance and Relationship Management Service

Table of Contents

List of Tables

Schedule A 4 – Governance and Relationship Management Service

1.0 Governance and Relationship Management Service Overview and Objectives

This Schedule sets forth the roles and responsibilities of the Parties under the Contract for the Governance and Relationship Management services provided under the Contract, as part of the Service Desk Services described in **Schedule A 1 – Service Desk Services**. Governance and Relationship Management Services are the services and activities, as further detailed in this Schedule, required to support the overall managed service relationship between Shared Services Canada (SSC) and the Contractor.

The Parties will, within sixty (60) FGWDs from Contact Award, agree to a series of performance measures (Service Level Requirements), Key Performance Indicators (KPIs) and relationship health check indicators that will be reported monthly and will record the performance of the relationship over the life of the Contract.

1.1 Governance and Relationship Management Service Objectives

SSC recognizes that Governance and Relationship Management Services are an essential element for successful contract management and ongoing SSC-Contractor relationship satisfaction. SSC requires a relationship with the Contractor that is based on the following key relationship characteristics, including:

- Mutual trust and respect;
- Excellent communication between both Parties;
- Well-defined objectives and service levels;
- Appropriate governance structures; and
- Well-defined roles and responsibilities covering the service management relationship.

1.2 Relationship Management Service Requirements

The Contractor must achieve the following relationship goals and objectives:

- Delivery of high-quality Service Desk Services to support SSC business needs and shared services requirements;
- High customer satisfaction from all End Users and Partner / Non-Partner Service Desk Agents using the Service Desk Services;
- Continuous recommendations on improvements to the functionality, development and delivery of Services to better meet SSC business objectives and customer requirements;
- Development of the business rationale and benefits of any proposed changes and communication of this information to the Service Desk teams and other SSC stakeholders, as appropriate;
- Working within the mutually-agreed structure regarding processes and procedures;
- Assisting SSC in its ongoing planning activities, as required; and
- Ensuring sufficient, efficient and continuous communication throughout the service relationship.

1.3 Day-to-Day Management

Reporting and communication processes will be documented and maintained by the Contractor, as approved by SSC.

The Contractor must provide additional points of contact and a reporting structure to support day-to-day operations and reviews of the Contractor's performance and contractual adherence. These reviews may include technical, financial, and service-level requirements, as well as resolution of operational issues.

Documentation must be maintained by the Contractor in an online repository accessible to the SSC management team. A regular meeting schedule must be established for the reporting levels outlined in this document, with access to all of the Contractor's defined points of contact based on 24-hours advance notice. In addition to the processes and procedures described in **Schedule A 1 – Service Desk Services** and **Schedule A 2 – Service Management Services**, the Contractor must provide processes and procedures acceptable to SSC that can be used to manage the day-to-day relationship. A comprehensive list of governance processes and procedures will be jointly defined by SSC and the Contractor as part of Transition services (**Schedule A 3 – Transition Services**).

2.0 Key Roles

The Contractor must establish and maintain a stable Relationship Management Team of senior IT and business professionals that, throughout the Contract lifecycle, will:

- Support SSC business objectives;
- Invest time and resource effort to act as a key enabler of the success of the relationship;
- Support SSC strategic and tactical planning processes for in-scope Services, including alignment with SSC's broader IT and business objectives, and its technology standards and architectures;
- Monitor the Contractor's performance metrics, including contracted SLR, KPIs and relationship health check indicators;
- Provide input and feedback to SSC leadership on opportunities to optimize its IT and business processes; and
- Adhere to established escalation managements procedures.

The Contractor must establish and provide the Management Team, including Key Contractor Personnel, such as those responsible for key projects, operations and technical management. The foregoing provisions are *in addition to*, not in lieu of, the provisions regarding Key Contractor Personnel set forth in the Contract. Key Contractor Personnel include, but are not limited to, the Contractor's staff described below.

To ensure consistency of service delivery and minimize personnel learning curves and disruptions, the Contractor agrees to minimize turnover in staff assigned to the SSC account (both Key and non-Key Personnel) to a mutually agreed level per Contract Year.

The Key Contractor Personnel identified for Transition related activities (see Section 2.4 Solution Architect, Section 2.5 Transition Manager, Section 2.6 Knowledge Transition Manager(s) and Section 2.7 Training Manager) must be engaged and available until the later of:

i. 90 days after successful cutover of all volumes;

ii. date upon which all services levels achieved for all volumes; or

iii. the discretion of SSC.

2.1 Client Executive

The Contractor must assign a Client Executive who is responsible for, but not limited to, the following:

- Acting as the primary Relationship Manager between the Contractor and SSC, ensuring the overall optimum health of all in-scope services and that all SOW requirements are met;
- Participating in the resolution of escalated Problems, Disputes, Incidents, and Service and Contract Changes;

- Working with SSC to address relevant high-level issues and proposing innovations and process improvements related to the Contract services in support of SSC strategic business transformation;
- Advocating for Partner / Non-Partner Service Desk Agents and End-users, as well as striving for improved client satisfaction and service delivery improvements; and
- Ensuring that all personnel designated with a Key Role in the SOW are knowledgeable about SSC's Service Lines, as well as the Contractor's and its subcontractors' own products and services.

The Contractor's Client Executive or his/her representative must have overall responsibility for directing all of the Contractor's activities as provided hereunder and must be vested by the Contractor with all necessary authority to act for the Contractor in connection with all aspects of the Contract.

2.2 Service Delivery Managers

The Contractor must designate individuals who will be the Contractor's primary point-of-contact for all matters relating to a specific scope of service. A specific manager must be identified for each of the Enterprise and End User Service Desk Services.

The Contractor Service Delivery Managers will be responsible for, but not limited to, the following:

- Acting as the Manager for services provided to SSC, ensuring the overall optimum health of all in-scope services and that all service requirements are met;
- Coordinating the resolution of escalated Problems, Disputes, Incidents, and Service and Contract Changes;
- Ensuring appropriate allocation and coordination of resources to meet service requirements;
- Ensuring that all front-line personnel are knowledgeable about SSC, the service environment, processes and procedures;
- Advocating for Partner / Non-Partner Service Desk Agents and End-users respectively, as well as striving for improved client satisfaction and service delivery improvements; and
- Being knowledgeable about SSC's Service Lines, and the Contractor's and its Subcontractors' own products and services.

2.3 Quality Assurance Manager

The Contractor must designate a Quality Assurance Manager who will provide a systematic approach, ongoing feedback, and ensure high and consistent level of support quality across all customer interactions of Service Desk services. The expected resource responsibilities must include, but are not limited to:

- Maintaining and developing Contractor's internal support and Service Desk quality standards;
- Reviewing a subset of Service Desk agents' interactions;
- Providing feedback on agent interactions, developing and delivering additional training as appropriate;
- Evaluating the QA team and investigating complaints or performance concerns;
- Investigating customers' needs and developing a strategy for meeting the requirements; and
- Analyzing all service metrics and how the Service Desk agent's performance affects those KPIs and create strategies to improve KPIs.

2.4 Solution Architect

The Contractor must designate an individual to ensure that the Enterprise Service Desk (ESD) and End User Service Desk (EUSD) are aligned with SSC's overall enterprise architecture guidelines and standards.

The Contractor Solution Architect will be responsible for the overall quality of deliverables from a technical aspect, including:

- Assessing SSC requirements and designing solutions that include service and technology components that support SSC's requirements and are technically sound and sustainable;
- Ensuring that technical design and implementation comply with SSC-established guidelines and standards;
- Ensuring consistency and integrity of technical approaches and the underlying interfaces (for example, integration with the Contractor's system(s) and SSC systems, as required)
- Periodically providing technical plans on how best to improve the efficiency and quality of the services; and
- Working directly with the SSC Solution Architect(s), who retains overall control of solution architecture.

2.5 Transition Manager

Each transition from one service state to another (e.g., initial transition, evolution of a service, introduction of a new service or transfer of a service), will require the establishment of a Transition Team, with membership from both Parties, to establish the new service state.

The Contractor must appoint a Transition Manager for the duration of the applicable transition period(s) to manage the transition.

The expected resource responsibilities must include, but are not limited to:

- Acting as the overall project manager to coordinate the Contractor's resources in transitioning SSC Service Desk Services to the new service arrangement;
- Coordinating with SSC's Project Director to plan and execute successful service transitions. The project plan will include, but not be limited to, an integrated Transition Project Plan for the Service Desk Services, a Work Breakdown Structure (WBS) and Schedule, a Risk Register, and an Issues List;
- Coordinating project meetings between SSC and the Contractor;
- Providing weekly Transition Project status reports and updates to SSC;
- Ensuring that Transition Project deliverables are on schedule and securing SSC's signoff for each milestone/deliverable;
- Ensuring that functionality of solution(s) and service requirements are met before SSC signoff is requested, including the full functionality of technology components of both Contractor- and SSC-provided technology; and
- Advocating for Non-Partner Service Desk Agents and End-users respectively, as well as striving for improved customer satisfaction and service delivery improvements.

2.6 Knowledge Transfer Manager(s)

The Knowledge Transfer Manager plays a key role that the Contractor must provide during a transition in order to establish innovative methods of knowledge collection and dissemination. In addition, the Knowledge Transfer Manager will be required to work with the counterpart SSC Knowledge Management function on an ongoing basis to capture, develop and maintain the knowledge base. The expected resource responsibilities will include, but are not limited to:

- Developing an effective and repeatable Knowledge Management process based on ITIL Standards and Knowledge Centered Support Standards;

- Facilitating cross-functional Knowledge Management process coordination with stakeholders;
- Establishing internal and cross-functional processes with SSC, such as for Incident resolution;
- Contributing to the authoring, maintenance and lifecycle for Knowledge Base content;
- Maintaining the Training Knowledge Base, Best Practice Tips, “How To’s”, and other publication sources in Self-Help; and
- Documenting as-is procedures in a manner that can facilitate redesigning and re-engineering Service Desk processes to enable ongoing IT service delivery performance.

2.7 Training Manager

The Contractor must designate a Training Manager who will provide training, communication, and support documentation for IT process, workflow, and Standard Operating Procedures (SOPs) for the transition, as it pertains to Service Desk Services. The expected resource responsibilities must include, but are not limited to:

- Creating, maintaining and continually evolving training material to support role based processes, tasks, and SOPs;
- Managing training material within the Service Desk Knowledge Database or document repository;
- Providing, managing, tracking and measuring Service Desk agents awareness and adoption for in-scope services;
- Planning, designing, and implementing effective, engaging, innovative, and interactive training activities;
- Contributing to the development, maintenance, quality of knowledge base. On regular intervals will participate in knowledge base reviews;
- Monitoring training compliance and continuous improvement; and
- Preparing periodic reports to communicate outcomes of training activities.

2.8 Performance Management Function

The Contractor must provide a Performance Management function that will have overall responsibility for ensuring that the Contractor’s performance meets SSC business requirements, and for recommending continuation of current practices, improvement of current practices or problem resolution to ensure that business requirements are met. The expected resource responsibilities will include, but are not limited to, the following:

- Leading assessment and development processes for measuring performance against SLRs;
- Reviewing and monitoring performance and facilitating development of improvement plans;
- Conducting exploratory activities to determine how to raise performance levels and recommending changes in SLRs, where appropriate, to ensure that they properly reflect business needs, while balancing costs; and
- SSC and the Contractor will review the KPIs performance semi-annually or in greater frequency as agreed between SSC and the Contractor. Any remediation and action items generated to address the KPI performance issues, and approved by SSC, will be implemented by the Contractor as part of the service improvement objective at no extra cost for SSC.

3.0 Governance Structure

The following Contract governance committee structure defines the framework of the participants, roles, responsibilities and activities responsible for the administration of the governance processes.

3.1 Service Desk Services Executive Committee

The Executive Committee will comprise senior executives from SSC and the Contractor (members to be determined) who will meet on a quarterly basis to discuss strategic and operational issues related to the Contract. The Executive Committee will be responsible for providing strategic direction to the Service Desk Services Contractor Operations Committee.

The Executive Committee will have the following roles and responsibilities:

- Addressing relevant high-level issues appropriate for executive-level discussion and decision-making;
- Reviewing and approving the use of innovation options (related to the Contract services) to support SSC strategic business improvement and transformation; and
- Reviewing the status of escalated Problems, Disputes, Incidents, and/or Service and Contract Changes.

At least five (5) FGWDs prior to the Executive Committee meeting, the Parties will agree on the meeting format, location, proposed agenda and required attendees.

3.2 Service Desk Services Operations Committee

The Service Desk Services Operations Committee will comprise business management and technology representatives from SSC and the Contractor. The Operations Committee will be responsible for overseeing the operation of Service Desk Services, reviewing performance and addressing issues. Issues that cannot be resolved by this Committee will be escalated to the Executive Committee.

The Operations Committee will be chaired by a senior SSC Manager. Committee membership must include Contractor Service Delivery Managers and/or Leads/Project Managers for each of the in-scope ESD and EUSD Services, in addition to the Contractor Project Executive. Any additional temporary or ad hoc Contractor attendees must be agreed by SSC in advance of the Operations Committee meetings.

The Operations Committee will meet monthly or more often at the request of SSC, and will have the following roles and responsibilities:

- Defining and recommending innovation and improvement opportunities for more effective use of Service Desk Services and driving cost-benefit analyses of the potential impact on those services;
- Presenting major opportunities (subject to pre-defined thresholds) to the Executive Committee while minor opportunities (subject to the same thresholds) will be presented and approved by this Committee;
- Addressing Problems, Disputes, Incidents and/or Requests for Changes;
- Reviewing the Contractor's overall performance with respect to SLRs for all Services, as well as credits and earn-backs based on SLR performance;
- Reviewing the Quality Assurance Scorecard;
- Reporting status of planned initiatives and discussing initiatives that may impact capacity requirements;
- Reviewing SSC satisfaction with the Key Contractor Personnel;
- Adjusting plans and projects as directed by SSC; and

- Reviewing and approving the Executive Management Report.

At least five (5) FGWDs prior to the Operations Committee meeting, the Parties will agree on the meeting format, location, proposed agenda and required attendees.

3.3 Service Management Team

For the Services defined in **Schedule A 1 – Service Desk Services** and **Schedule A 2 – Service Management Services**, the joint Service Management Team, comprising business management and technology staff from SSC and the Contractor, will be responsible for overseeing the day-to-day operation of the in-scope Service Desk Services.

Service Management Team meetings will be chaired by SSC. Its members will include the Contractor Service Delivery Manager for the associated Services, plus any additional key Contractor attendees that are required, as agreed with SSC. Any additional temporary or ad hoc Contractor attendees must be agreed with SSC in advance of Service Management Team meetings.

The Service Management Team will meet on a weekly or other basis, to be agreed between the associated Contractor Service Delivery Manager and the SSC Technical Authority, and will have the following roles and responsibilities:

- Addressing operational and/or delivery issues and/or crises arising during the previous week, and their impacts on SLRs;
- Reviewing the Root Cause Analysis of any previous issues;
- Addressing outstanding or unresolved issues;
- Reviewing progress reports;
- Planning for future changes;
- Reviewing the Contractor's compliance with the SLRs;
- Reviewing Payment Credits to be applied;
- Reviewing Problems, Disputes, Incidents and Change Requests; and
- Addressing such other matters as one Party may bring to the attention of the other.

At least five (5) FGWDs prior to the Service Management Team meeting, the Parties will agree on the meeting format, location, proposed agenda and required attendees.

4.0 Governance Processes

The Contractor must collaborate with SSC and participate in managing the governance processes in support of the relationship as outlined below:

- Change Management;
- Client Satisfaction Management;
- Dispute Resolution;
- Integration Management;
- Performance Reporting such as SLRs, project status, outstanding service request status;
- Resource Management;

- Service Level Management;
- Heightened Awareness Window;
- Strategy and Planning; and
- Financial Management including ARC/RCC Management.

These processes will be defined in Transition Services within 60 FGWDs of Contract Award. The Contractor must assign an owner of the day-to-day operations and management of the governance processes to satisfy SSC service requirements.

Schedule B 3 – Financial Responsibility Matrix defines the prime responsibilities (either the Contractor or SSC) for both hardware and software assets.

4.1 Governance and Relationship Management Roles and Responsibilities

The following table identifies the roles and responsibilities associated with Governance and Relationship Management that the Parties must perform. Any approval and/or review will be the responsibility of SSC.

Table 49: Governance and Relationship Management Roles and Responsibilities

Identifier	Governance and Relationship Management Roles and Responsibilities	Contractor	SSC
Strategy and Planning			
1.01	Participate in quarterly Executive Committee meetings.	X	
1.02	Provide strategic business and technology imperatives that require Contractor support.		X
1.03	Provide status on current and proposed projects (if applicable).	X	
1.04	Recommend services, technologies, products and and/or leading practices from comparable/peer engagements that could add value to SSC and its services.	X	
1.05	Review and submit for approval projects and project plans (as applicable).	X	
1.06	Participate in the development of strategic business plans, as requested by SSC.	X	
1.07	Develop/implement operational plans in accordance with the authorized strategic IT Plan, architecture and implementation strategies.	X	
1.08	Provide IT research assistance on new technologies.	X	
1.09	Provide business case inputs and support preparation, as required.	X	
1.10	Provide IT solutions, expertise, and advisory services that are appropriately aligned with SSC's needs and business focus.	X	
1.11	Establish business criteria for all services, standards and delivery requirements.		X
1.12	Recommend appropriate services, standards and procedures.	X	
1.13	Submit for review and approval all recommended services, standards and procedures.	X	
1.14	Approve all recommended services, standards and procedures.		X
1.15	Adhere to GC and SSC Policies and Standards.	X	
1.16	Develop, document and maintain Service Delivery Manual.	X	
1.17	Submit for approval Service Delivery Manual.	X	
1.18	Approve Service Delivery Manual.		X
1.19	Provide the Service Delivery Manual electronically (and in a manner such that it can be accessed via either the SSC Intranet or the Internet).	X	
1.20	Communicate to SSC the availability of and methodology for accessing the Service Delivery Manual.	X	
1.21	Manage and coordinate all delivery aspects of the Services.	X	

Identifier	Governance and Relationship Management Roles and Responsibilities	Contractor	SSC
Service Level Management			
1.22	Provide regular written performance management reports to SSC on SLRs and conduct periodic scheduled and ad hoc review meetings as required.	X	
1.23	Monitor and submit for review the Contractor's performance against SLRs, performance improvement plans and industry benchmarks.	X	
1.24	Ensure Contractor understanding of and adherence to SLRs and implementations of any required changes to achieve such SLRs.	X	
1.25	Ensure in-scope technical solutions are consistent with SSC business strategy and architecture.	X	
1.26	Ensure Contractor performance meets business requirements.	X	
1.27	Conduct a formal review and report on root causes of service delivery or other relationship-related matters, and document such findings per the requirements in **Schedule A 1 – Service Desk Services** and **Schedule A 2 – Service Management Services**.	X	
1.28	From time to time, conduct reviews/checks to ensure the contractual commitments are being met, and ensure there is no violation to contractual obligations, including legal-, security- and compliance-related requirements.		X
1.29	Close any gaps identified during reviews, audits and compliance checks and assist audits and compliance requirements.	X	
Resource Management			
1.30	Execute the reviewed Human Resources Sourcing and Retention Strategy.	X	
1.31	Ensure that staffing, technology and skill levels are adequate to achieve contract objectives.	X	
1.32	Ensure that staff have certified bilingual capability necessary to provide high-quality Service Desk Services.	X	
1.33	Inform SSC of any potential key personnel staffing changes and of any new personnel assignments planned for new projects and Services.	X	
1.34	Review and authorize key personnel changes to existing Services and personnel for new projects and Services.		X
1.35	Adhere to any defined constraints on the use of subcontractors.	X	
1.36	Recommend subcontractors for delivery of Services, if applicable.	X	
1.37	Establish, maintain and provide a register of all sub-contracts relevant to the Services in the Contract.	X	
1.38	Provide Contractor staff turnover data.	X	
Service Integration Management			
1.39	Provide information on service integration requirements.		X
1.40	Define service integration solutions.	X	
1.41	Submit for approval defined service integration solutions.	X	
1.42	Develop/recommend overall IT architecture, implementation strategies and subcontractor integration strategies for in-scope Services in support of the SSC Strategic IT Plan.	X	
1.43	Submit for Review and approval the IT architecture, implementation strategies and subcontractor integration strategies for in-scope Services.	X	
1.44	Participate in operational governance processes between SSC and the Contractor, as required.	X	
1.45	Support development and document Operating Level Agreements (OLAs) between SSC / other government organizations, subcontractors and the Contractor, if subcontractors are providing services that integrate or impact upon those defined in the Contract.	X	
1.46	Develop OLAs between SSC / other government organizations, subcontractors and the Contractor, if subcontractors are providing services that integrate or impact upon those defined in the Contract.		X

Identifier	Governance and Relationship Management Roles and Responsibilities	Contractor	SSC
Customer Satisfaction Management			
1.47	Provide regular written performance management reports to SSC on SLRs and conduct regular scheduled and ad hoc review meetings as required.	X	
1.48	Conduct ongoing customer satisfaction surveys.	X	
1.49	Participate in and review customer satisfaction surveys.		X
Heightened Awareness Window			
1.50	Participate in a “war room” gathering for concentrated focus to ensure that technical teams respond quickly in the event of an incident.	X	
1.51	Lead the HAW process		X
1.52	The application or service is added to the CBAS list by the Incident Management (IM) team for the approved period of time		X
1.53	Define the support period (i.e. 24x7, Monday-Friday 8:00 to 16:00, 9:00-17:00)		X
1.54	Responsible for Incident Notification (INOT), Executive Notification (ENOT) and Critical Incident Summary (CIS) for Critical Priority Incidents		X
1.55	Dedicated management and/or supervisor level resources to participate in the HAW	X	

Schedule A 5 – High Level Design with Security Controls

Shared Services Canada (SSC)

Schedule 5 – High Level Design

Table of Contents

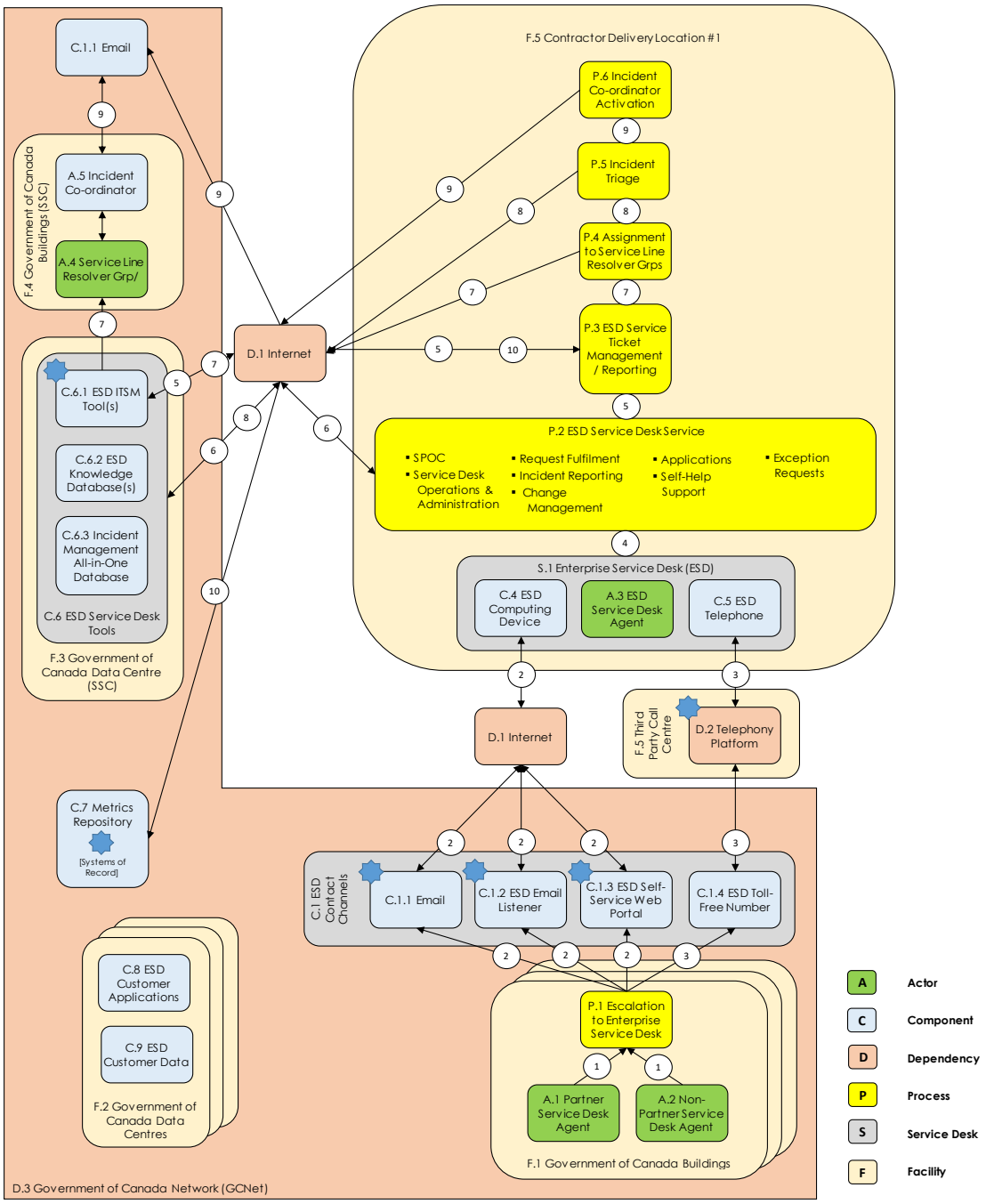
List of Figures

List of Tables

Schedule 5 – High Level Design

1.0 Logical Architecture

This section describes the Logical Architecture of the Enterprise Service Desk (ESD) and End User Service Desk (EUSD). The architecture is described in terms of logical components from the conceptual architecture as well as dependencies, processes and actors.



1. Partner / Non-partner Service Desk Agents identifies incident report or service request requiring escalation to the ESD
2. Partner / Non-partner Service Desk Agent escalates incident or requests service from computing device via available channels (email/email listener/self-service web portal/chat)
3. Partner / Non-partner Service Desk Agent escalates incident or requests service from telephone
4. ESD Service Desk Agent identifies service required
5. ESD Service Desk Agent takes information and logs ticket in ESD ITSM Tool
6. ESD Service Desk Agent attempts to resolve incident, fulfill request or execute change request using ESD Knowledge Database(s)
7. ESD Service Desk Agent determines that issue cannot be resolved or request cannot be fulfilled - assigns to Service Line Resolver Group using ESD ITSM Tool
8. ESD Service Desk Agent uses Incident Management All-in-One tool to triage incident (Low, Medium, High, Critical, High Availability Window (HAW))
9. ESD Service Desk Agent "IC Activates" via Email to Incident Co-ordinator for High, Critical and HAW Incidents
10. Contractor extracts raw transactional data from Systems of Record on a daily/weekly/monthly basis and stores in Data Warehouse

Figure 1: ESD Logical Architecture

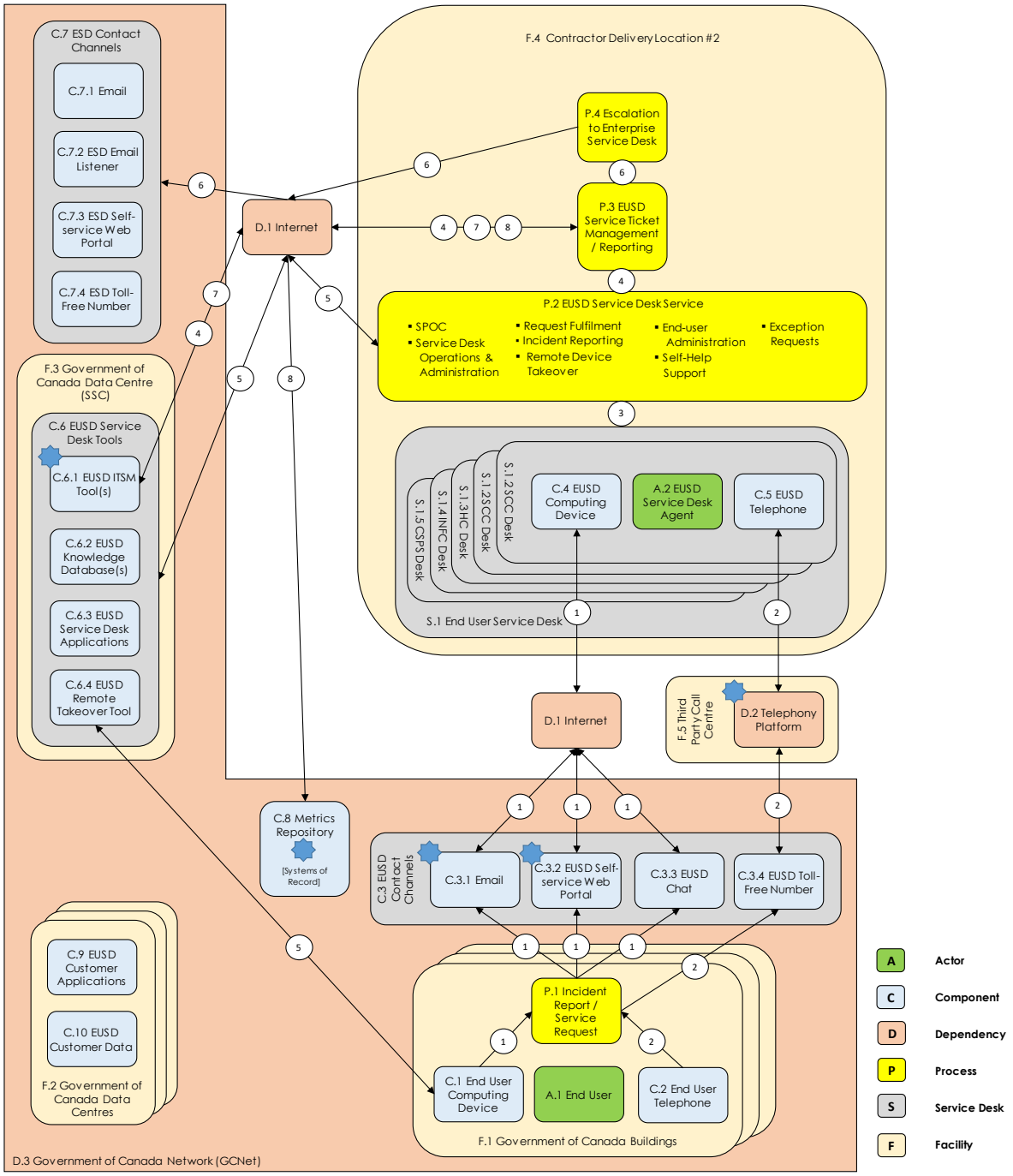
Table 50: Elements of ESD Logical Architecture

Actor Identifier	Actor Name	Actor Descriptions	Schedule
A.1	Partner Service Desk Agent	Service Desk Agents employed by Partner Service Desks (end user service desks for Partner Departments). Partner Departments are mandated to consume SSC Provided Enterprise Services.	A 7 / A 12
A.2	Non-Partner Service Desk Agent	Service Desk Agents employed by Non-Partner Service Desks (end user service desks for Non-Partner Clients). Non-Partner Clients are those Government of Canada agencies/organizations consuming limited Enterprise Services.	A 7 / A 12
A.3	ESD Service Desk Agent	Contractor Personnel providing Single Point of Contact Services for ESD Customers.	A 1 / A 7
A.4	Service Line Resolver Group	Government of Canada employees or contractors tasked with resolving issues impacting services provided by their service line	A 7 / A 16
A.5	Incident Coordinator	Government of Canada employees or contractors with responsibility for incident management relating to High, Critical or HAW events.	A7
Component Identifier	Component Name	Component Descriptions	Schedule
C.1	ESD Contact Channels	Four channels are available to allow Partner Service Desk Agents / Non-Partner Service Desk Agents to contact the Enterprise Service Desk: a) Email b) ESD Email Listener c) ESD Self-service Web Portal d) ESD Toll-Free Number	-
C.1.1	Email	Electronic Email service provisioned by the Government of Canada.	-
C.1.2	ESD Email Listener	The custom application which operates as a bridge between ESD ITSM Tool(s) and ITSM Tool(s) used by ESD Customers.	A 7 / B 3
C.1.3	ESD Self-Service Web Portal	Service Government Service Catalog Portal (SGSC)	B 3
C.1.4	ESD Toll-Free Number	Government of Canada provided Toll-Free Number.	A 12
C.4	ESD Computing Device	Enterprise Service Desk Computing Device provisioned and imaged by the Contractor.	A 1 / B 3
C.5	ESD Telephone	Enterprise Service Desk Telephone/Headset provisioned by the Contractor.	A 1 / B 3

C.6	ESD Service Desk Tools	The Enterprise Service Desk uses multiple Service Desk Tools as follows:
		a) ESD ITSM Tool(s);
		b) ESD Knowledge Database(s);
		c) Service Desk Applications;
			B 3

C.6.1	ESD ITSM Tool(s)	Information Technology Service Management (ITSM) tool(s) provisioned by SSC and used to create and track reported incidents and service requests for ESD Customers	A 7 / B 3
C.6.2	ESD Knowledge Database(s)	Knowledge Database(s) provisioned by SSC.	B 3
C.6.3	Incident Management All-in-One Database	Database used by ESD Service Desk Agents to triage incidents.	B 3
C.7	Metrics Repository	Metrics repository provisioned by SSC and maintained by the Contractor to store raw transactional data from Systems of Record.	B 4
C.8	ESD Customer Applications	ESD Customer enterprise applications hosted in Government of Canada Data Centres.	A 13
C.9	ESD Customer Data	ESD Customer data repositories located Government of Canada Data Centres.	-
Dependency Identifier	Dependency Name	Dependency Descriptions	Schedule
D.1	Internet	Internet access is required for remote access to the WAN (GCNet).	-
D.2	D.2 Telephony Platform	Telephony platform provided by the Government of Canada	A 1 / B 3
D.3	Government of Canada Network (GCNet)	WAN Component of the SSC Network.	-

Facilities Identifier	Facilities Name	Facilities Descriptions	Schedule
F.1	Government of Canada Buildings	Government of Canada building(s) accommodating employees/contractors of ESD Customers.	-
F.2	Government of Canada Data Centres	Government of Canada building(s) hosting ESD Customer Applications and ESD Customer Data.	-
F.3	Government of Canada Data Centre (SSC)	Government of Canada building(s) hosting ESD Service Desk Tools.	-
F.4	Government of Canada Data Buildings (SSC)	Government of Canada building(s) hosting Service Line Resolver Groups and Incident Coordinators.	-
F.5	Contractor Delivery Location #1	Delivery Location provided by the Contractor from which the ESD Service Desk Services are provided.	
Process Identifier	Process Name	Process Descriptions	
P.1	Escalation to Enterprise Service Desk	Process for escalating unresolvable incidents to the Enterprise Service Desk.	A 16
P.2	ESD Service Desk Service	Service Desk Services include the following services: a) Single Point of Contact (SPOC) Service; b) Service Desk Operations and Administration Service; c) Request Fulfilment Service; d) Incident Reporting Service; e) Change Management Service; f) Application Service; f) Self-Help Support Service; g) Exception Requests.	A 1
P.2.1	Single Point of Contact (SPOC) Service	The Single Point of Contact Services provides toll-free support and electronic ticketing for logging, tracking, Resolution and reporting of Service Desk Incidents and Service Requests for all Department of Justice Canada-supported environments.	A 1
P.2.2	Service Desk Operations & Administration Service	Service Desk Operations and Administration Services are the activities associated with providing a stable Service Desk environment and to effectively and efficiently perform procedures to ensure IT Services meet SLR targets and requirements.	A 1
P.2.3	Request Fulfilment Service	Request Fulfilment Services are the activities associated with the fulfilment of Service Requests.	A 1
P.2.4	Incident Reporting Service	Incident Reporting Services are the activities associated with Incident Reporting processes including escalation to the Enterprise Service Desk through a defined process.	A 1
P.2.4	Change Management Service	Change Management Services are the activities associated with identifying the various tasks of the Contractor and SSC for dealing with change management requests.	A 1
P.2.5	End-User Administration Service	End-User Administration Services are the activities associated with managing and coordinating account creation, activation, termination, Changes and expiration.	A 1
P.2.6	Self-Help Support Service	Self-Help Support Services are the activities associated with IVR capabilities, out of prime-time (voice messaging with guaranteed call-back response), intranet based automated self-help support, etc.	A 1
P.2.7	Exception Request Service	Exception Requests Services are the activities associated with fulfilling End-User requests for products or Services that are outside the scope of the Services.	A 1
P.2.8	Application Services	Application Services are the activities associated with identifying the various tasks of the Contractor and SSC for dealing with application-related Incidents and Requests	A 1
P.3	ESD Service Ticket Management / Reporting	ESD Service Ticket Management / Reporting incorporates both C.6.1 ESD ITSM Tool(s) and D.2 Telephony Platform functionality to manage and report on ESD activities and performance.	A 1
P.4	Assignment to Service Line Resolver Groups	Where ESD Service Desk Agent determines that issue cannot be resolved or request cannot be fulfilled - assigns to Service Line Resolver Group using ESD ITSM Tool(s).	-
P.5	Incident Triage	Determines incident priority (Low, Medium, High, Critical, High Availability Window (HAW))	-
P.6	Incident Coordinator Activation	Provides Incident Co-ordination with Email notification that an incident with High, Critical or HAW has been assigned in the ITSM Tool(s)	-



1. End User reports incident or requests service from computing device via available channels (email/self-service web portal/chat)
2. End User reports incident or requests service from telephone
3. EUSD Service Desk Agent identifies service required
4. EUSD Service Desk Agent takes information and logs ticket in EUSD ITSM Tool
5. EUSD Service Desk Agent attempts to resolve incident or fulfill request using EUSD Knowledge Database(s), Service Desk Applications (resets) or Remote Takeover Tool
6. EUSD Service Desk Agent determines that issue cannot be resolved or request cannot be fulfilled - escalates to ESD through Email, Email Listener, Self-Service Portal or Telephone
7. EUSD Service Desk Agent updates ITSM Tool(s) reflecting resolution or escalation to ESD
8. Contractor extracts raw transactional data from Systems of Record on a daily/weekly/monthly basis and stores in Data Warehouse

Figure 2: EUSD Logical Architecture

Table 51: Elements of EUSD Logical Architecture

Actor Identifier	Actor Name	Actor Descriptions	Schedule
A.1	End User	Employees and contractors employed by EUSD Customers. EUSD Customers are the five departments for which SSC provides end-user support. End-users contact the EUSD for desktop environment related issues.	A 7 / A 12
A.2	Service Desk Agent	Contractor Personnel providing Single Point of Contact Services for EUSD Customers.	A 1 / A 7
Component Identifier	Component Name	Component Descriptions	Schedule
C.1	End User Computing Device	End User Service Desk Computing Device provisioned and imaged by the Government of Canada.	-
C.2	End User Telephone	Telephones provided to Government of Canada employees / contractors.	-
C.3	EUSD Contact Channels	Four channels are available to allow end-users to contact the End User Service Desk: a) Email; b) EUSD Self-service Web Portal; c) EUSD Chat; d) EUSD Toll-Free Number.	-
C.3.1	Email	Electronic Email service provisioned by the Government of Canada.	-
C.3.2	EUSD Self-Service Web Portal	Web-based interface through which users can submit incident and service requests, check the status of previously submitted requests, reset their password, etc.	-
C.3.3	EUSD Chat	Chat channel provisioned by the Government of Canada.	-
C.3.4	EUSD Toll-Free Number	Toll-Free number(s) provisioned by the Government of Canada for End Users to Contact the EUSD.	A 12
C.4	EUSD Computing Device	End User Service Desk Computing Device provisioned and imaged by the Contractor.	A 1 / B 3
C.5	EUSD Telephone	End User Service Desk Telephone/Headset provisioned by the Contractor.	A 1 / B 3

C.6	EUSD Service Desk Tools	The End User Service Desk uses multiple Service Desk Tools as follows:
		a) EUSD ITSM Tool(s);
		b) EUSD Knowledge Database(s);
		c) EUSD Service Desk Applications;
		d) EUSD Remote Takeover Tool.
			-

C.6.1	EUSD ITSM Tool(s)	Information Technology Service Management (ITSM) tool(s) provisioned by SSC and used to create and track reported incidents and service requests for EUSD Customers	A 7 / B 3
C.6.2	EUSD Knowledge Database(s)	Knowledge Database(s) provisioned by SSC.	B 3
C.6.3	Service Desk Applications	Service Desk Applications (i.e. resets) provisioned by SSC.	B 3
C.6.4	Remote Takeover Tool	Remote Takeover Tool(s) provisioned by the Government of Canada	B 3
C.7	ESD Contact Channels	Four channels are available to allow Partner / Non-Partner Service Desk Agents to contact the Enterprise Service Desk: a) Email; b) ESD Email Listener; c) ESD Self-service Web Portal; d) ESD Toll-Free Number.	-
C.7.1	Email	Electronic Email service provisioned by the Government of Canada.	-
C.7.2	ESD Email Listener	The custom application which operates as a bridge between ESD ITSM Tool(s) and ITSM Tool(s) used by ESD Customers.	A 7 / B 3
C.7.3	ESD Self-Service Web Portal	Service Government Service Catalog Portal (SGSC)	B 3
C.7.4	ESD Toll-Free Number	Government of Canada provided Toll-Free Number.	A 12
C.8	Metrics Repository	Metrics repository provisioned by SSC and maintained by the Contractor to store raw transactional data from Systems of Record.	B 4

C.9	EUSD Customer Applications	EUSD Customer enterprise applications hosted in Government of Canada Data Centres.	A 13
C.10	EUSD Customer Data	EUSD Customer data repositories located Government of Canada Data Centres.	-
Dependency Identifier	Dependency Name	Dependency Descriptions	Schedule
D.1	Internet	Internet access is required for remote access to the WAN (GCNet).	-
D.2	D.2 Telephony Platform	Telephony platform provided by the Government of Canada	A 1 / B 3
D.3	Government of Canada Network (GCNet)	WAN Component of the SSC Network.	-
Facilities Identifier	Facilities Name	Facilities Descriptions	Schedule
F.1	Government of Canada Buildings	Government of Canada building(s) accommodating employees/contractors of EUSD Customers.	-
F.2	Government of Canada Data Centres	Government of Canada building(s) hosting EUSD Customer Applications and EUSD Customer Data.	-
F.3	Government of Canada Data Centre (SSC)	Government of Canada building(s) hosting EUSD Service Desk Tools.	-
F.4	Contractor Delivery Location #2	Delivery Location provided by the Contractor from which the EUSD Service Desk Services are provided.	-
F.5	Third Party Contact Centre	Location of Hosted Contact Center Services	-
Process Identifier	Process Name	Process Descriptions	Schedule
P.1	Incident Report / Service Request	Process for end-users of EUSD Customers to report incidents and request services.	-
P.2	EUSD Service Desk Service	Service Desk Services include the following services: a) Single Point of Contact (SPOC) Service; b) Service Desk Operations and Administration Service; c) Request Fulfilment Service; d) Incident Reporting Service; e) Remote Device Takeover Service; f) Application Service; g) End-User Administration Service; h) Self-Help Support Service; i) Exception Requests.	A 1
P.2.1	Single Point of Contact (SPOC) Service	The Single Point of Contact Services provides toll-free support and electronic ticketing for logging, tracking, Resolution and reporting of Service Desk Incidents and Service Requests for all Department of Justice Canada-supported environments.	A 1
P.2.2	Service Desk Operations & Administration Service	Service Desk Operations and Administration Services are the activities associated with providing a stable Service Desk environment and to effectively and efficiently perform procedures to ensure IT Services meet SLR targets and requirements.	A 1
P.2.3	Request Fulfilment Service	Request Fulfilment Services are the activities associated with the fulfilment of Service Requests.	A 1
P.2.4	Incident Reporting Service	Incident Reporting Services are the activities associated with Incident Reporting processes including escalation to the Enterprise Service Desk through a defined process.	A 1
P.2.5	Remote Device Takeover	Remote Device Takeover Services are the activities associated with managing, maintaining and troubleshooting devices remotely over the network to minimize the need to dispatch technical personnel for Incident Resolution.	A 1
P.2.6	Application Services	Application Services are the activities associated with identifying the various tasks of the Contractor and SSC for dealing with application-related Incidents and Requests	A 1
P.2.7	End-User Administration Service	End-User Administration Services are the activities associated with managing and coordinating account creation, activation, termination, Changes and expiration.	A 1
P.2.7	Self-Help Support Service	Self-Help Support Services are the activities associated with IVR capabilities, out of prime-time (voice messaging with guaranteed call-back response), intranet based automated self-help support, etc.	A 1
P.2.8	Exception Request Service	Exception Requests Services are the activities associated with fulfilling End-User requests for products or Services that are outside the scope of the Services.	A 1
P.3	EUSD Service Ticket Management / Reporting	EUSD Service Ticket Management / Reporting incorporates both C.6.1 ITSM Tools and D.2 Telephony Platform functionality to manage and report on EUSD activities and performance.	A 1

P.4	Escalation to Enterprise Service Desk	Process for escalating unresolvable incidents to the Enterprise Service Desk.	A 16
Service Desk Identifier	**Service Desk Name**	**Service Desk Descriptions**	**Schedule**
S.1	End User Service Desk	Through dedicated "sub" desks, the End User Service Desk (EUSD) delivers end-user support to the following departments: a) Shared Services Canada (SSC); b) Public Service and Procurement Canada (PSPC); c) Canada School of the Public Service (CSPS); d) Infrastructure Canada (INFC); e) Health Canada (HC).	-
S.1.1	SSC Desk	Dedicated "sub" desk delivering end-user support to services to Shared Services Canada	-
S.1.2	PSPC Desk	Dedicated "sub" desk delivering end-user support to services to Public Service and Procurement Canada	-
S.1.3	CSPS Desk	Dedicated "sub" desk delivering end-user support to services to Canada School of Public Service	-
S.1.4	INFC Desk	Dedicated "sub" desk delivering end-user support to services to Infrastructure Canada	-
S.1.5	HC Desk	Dedicated "sub" desk delivering end-user support to services to Health Canada	-

2.0 High Level Design

The high-level designs for the ESD and EUSD, which can be seen in Figures 1 and 2, consist of the following security zones:

- Public Zone (PZ) – The Public Zone is entirely open and includes public networks such as the public Internet, the public switched telephone network, and other public carrier backbone networks and services[1]. The PZ is used to provide the necessary communications between Government of Canada Buildings/Data Centres and the Contractor's Facilities;
- Public Access Zone (PAZ) – A PAZ mediates access between operations zones of the Contractor Facilities and the Public Zone.[2]
- Operations Zone (OZ) – An OZ is the standard environment for routine Government of Canada operations. It is the environment in which most end-user systems and workgroup servers are installed.[3] The Government of Canada buildings and the Contractor Facilities have a separate OZ.
- Restricted Zone – a network security zone appropriate for critical applications (see App-RZ) and data (see DB-RZ), as well as for management workstations:
    - Application Restricted Zone – network security zone for mission-critical applications
    - Database Restricted Zone – network security zone for sensitive and/or critical data stores

ZIPs (shown) will be implemented between all zones. A ZIP provides a network interface between a zone and another zone. ZIPs are the logical constructs used to describe the controlled interfaces connecting the zones. ZIPs enforce zone data communication policy through perimeter security measures.[4] A PZ ZIP is used to control all types of traffic between the PZ and the PAZ. The PZ ZIP should be capable of filtering packets based on defined characteristics. The Public Zone ZIP hides the details of the network services

[1] ITSG-22
[2] ITSG-22
[3] ITSG-22
[4] ITSG-38

from the PZ and presents only those services necessary for communications with the PZ. An Internal Zone ZIP is used to control and filter all traffic between the PAZ and internal Zones. The Internal Zone ZIP should be capable of filtering packets based on defined characteristics. It should support the implementation of proxy services. The Internal Zone ZIP should be capable of rejecting all malformed service requests. It hides the details of the PAZ network services from the Internal Zones and presents only those services necessary for communications with Internal Zones. [5]

This section describes the High Level Design of the Enterprise Service Desk (ESD) and End User Service Desk (EUSD).

[5] ITSG-22

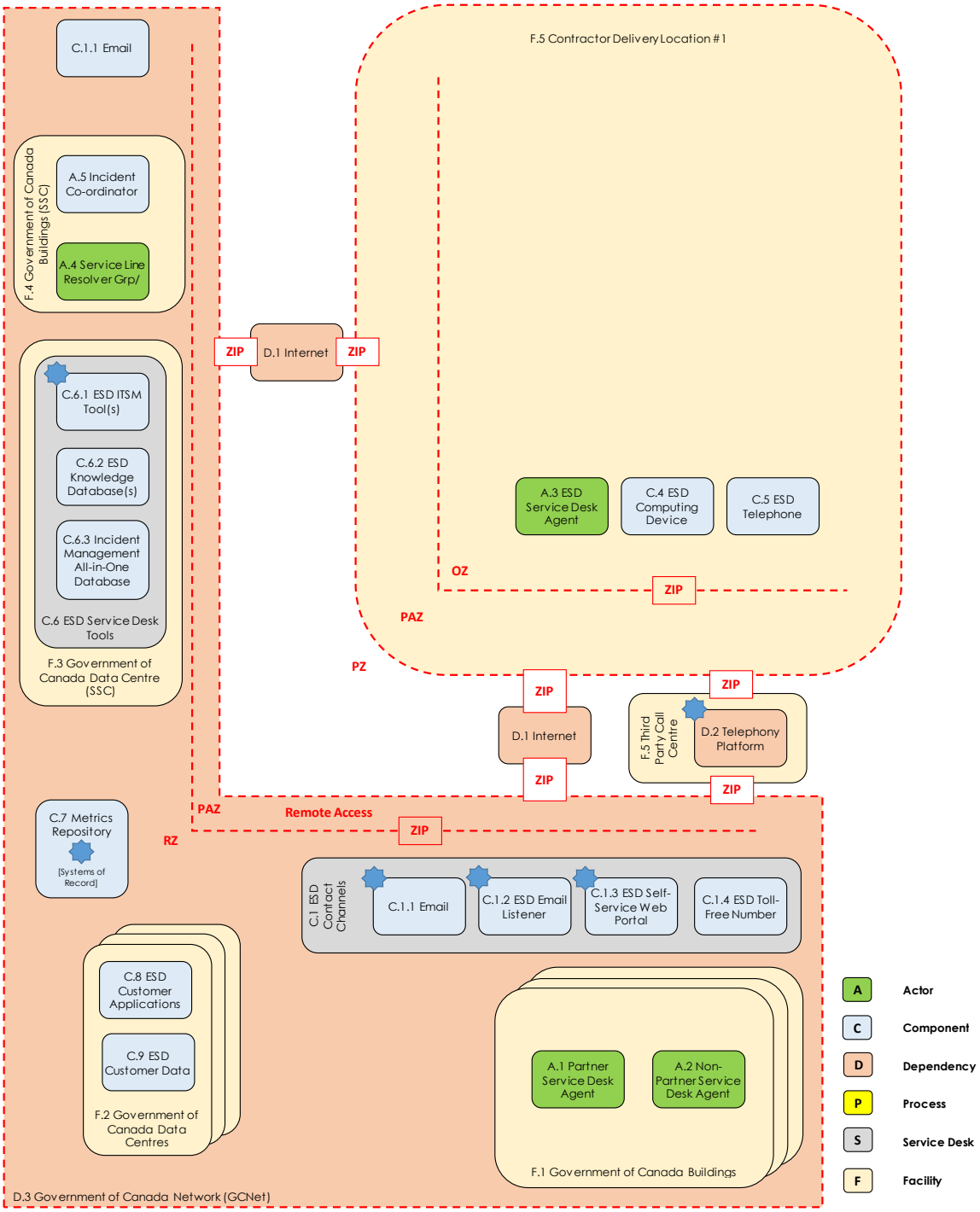


Figure 3: ESD High Level Design

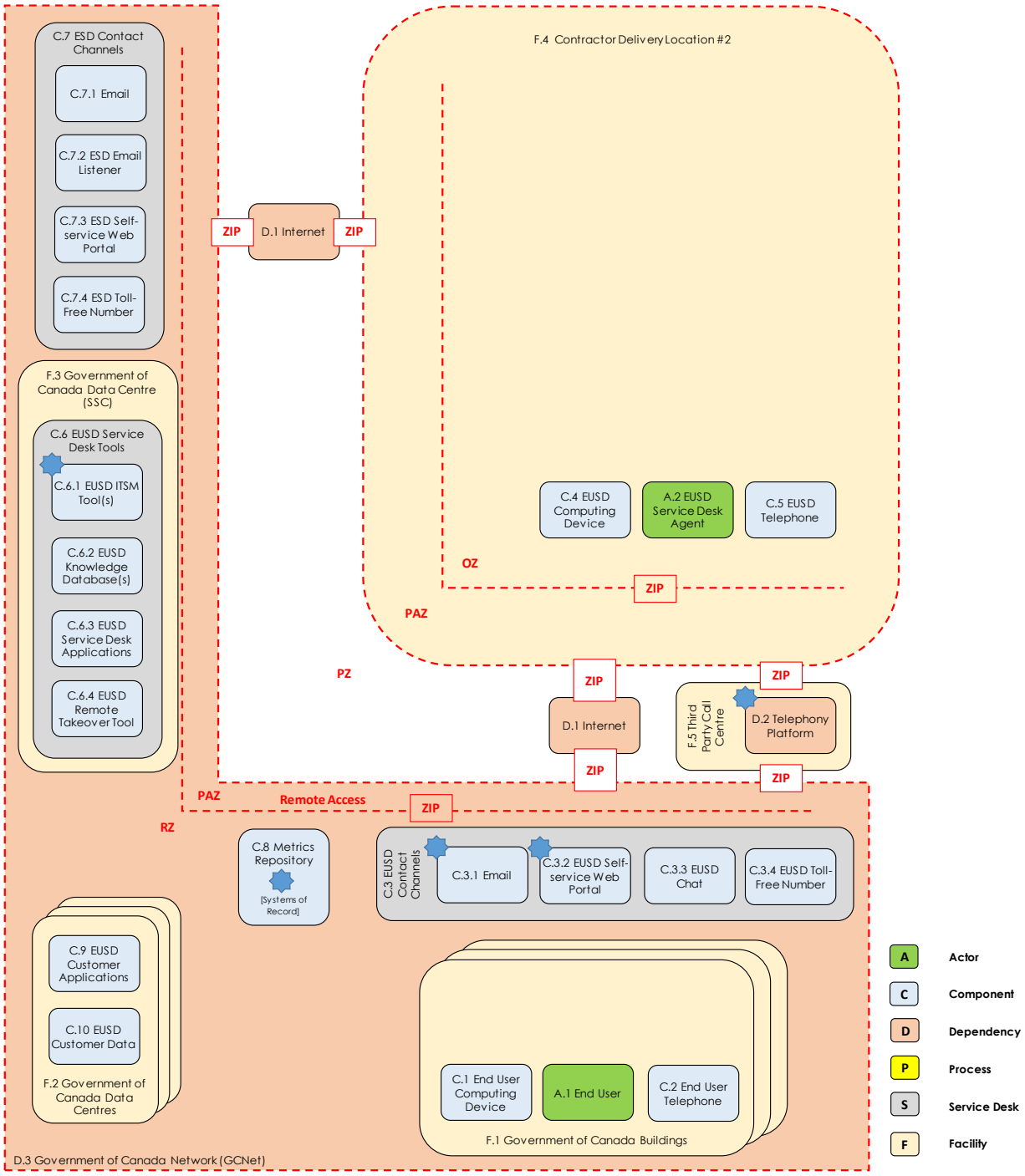


Figure 4: EUSD High Level Design

2.1 High Level Design with Security Controls

The high-level design for the Service Desk Project, which is described in Section 1.2, has been modified to include the key Contractor security controls and enhancements. The high-level design with security controls can be seen in Figures 5 and 6, below. The complete mapping of ITSG-33 security controls can be found in the Security Requirement Traceability Matrix (SRTM), which accompanies this document (see **Schedule A 6 – Security Requirements Traceability Matrix**). Six columns (i.e., F through K) are provided in the SRTM, to cover the content of each of the red boxes in Figures 5 and 6, in order to indicate where the security control should be applied.

It should be noted that the PBMM profile has approximately 169 security controls and 266 enhancements. Rather than present Bidders with approximately 435 security controls/enhancements it was decided to focus on key security controls and enhancements, and indicate where within the HLD they should be applied. The end result was a total of approximately 93 security controls/enhancements for each of the ESD and EUSD. While the key security controls and enhancements have been identified, the Contractor facilities, process and infrastructure are expected to operate in a manner consistent with, and conforming to, the security controls identified in the PBMM profile (profile 1) of ITSG-33.

It is also worth mentioning that all of the security controls and enhancements included in the SRTM, including the definitions (column D) and placeholder values (column E), have been extracted from the ITSG-33 Security Control Catalogue and the Suggested Security Controls and Control Enhancements documents found at https://www.cse-cst.gc.ca/en/publication/itsg-33 The text has not been modified in any way.

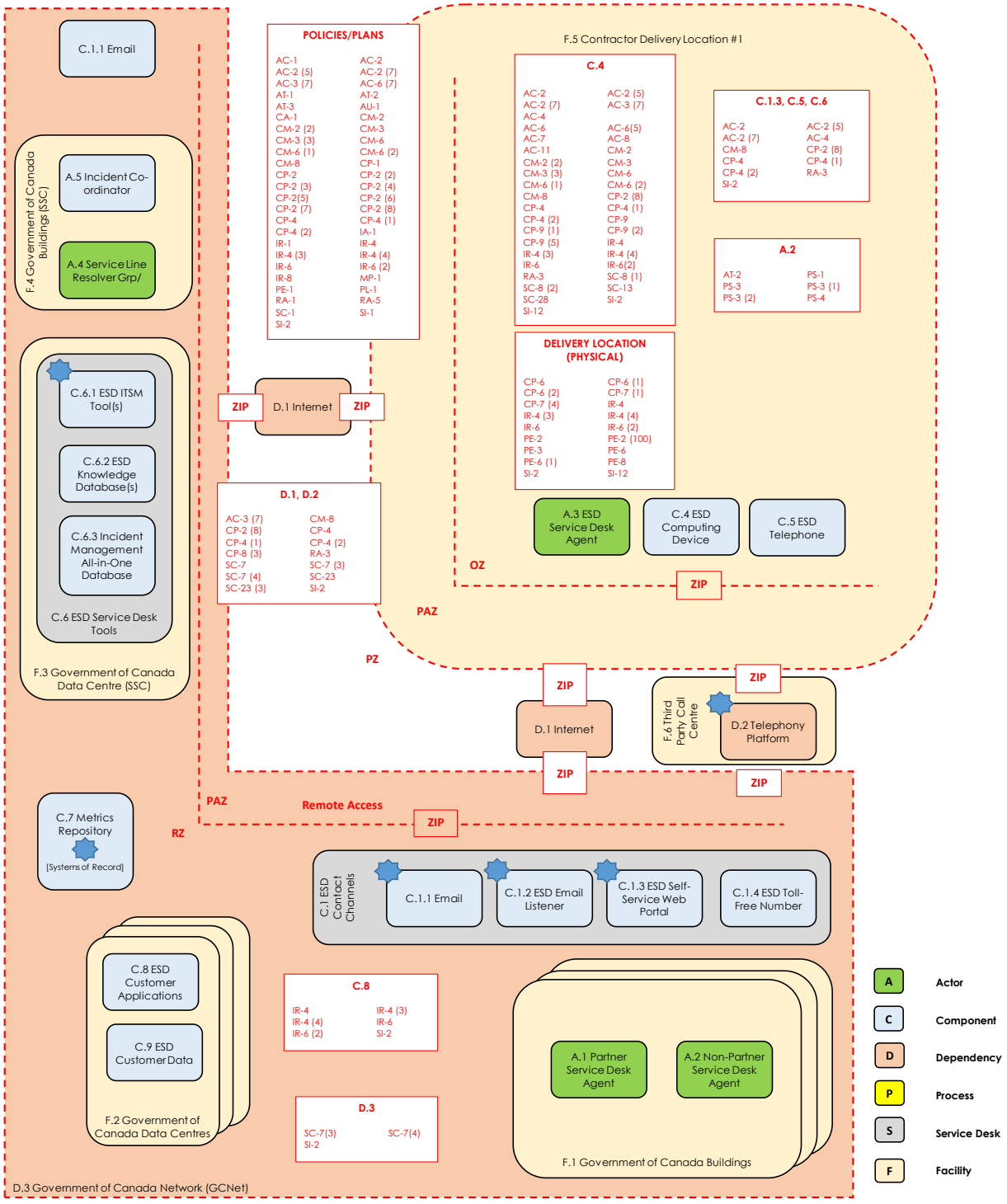


Figure 5: ESD High Level Design with Security Controls

Refer to the Government of Canada Communications Security Establishment document "ITSG-33, Annex 3A; Information Technology Security Guidance -- IT Security Risk Management: A Lifecycle Approach, Security Control Catalogue" for definition of the security controls noted in the above Figure 5.

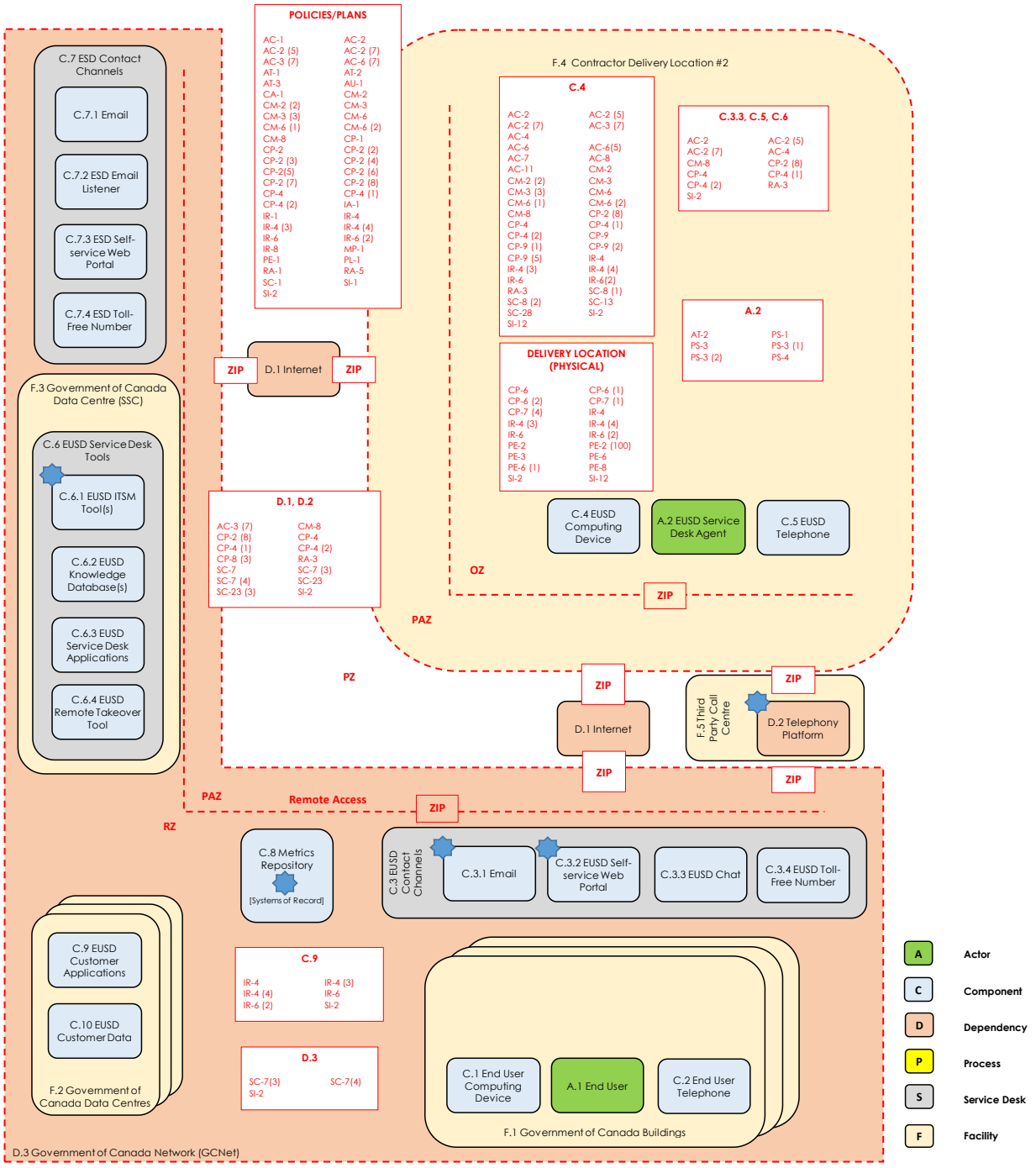


Figure 6: EUSD High Level Design with Security Controls

Refer to the Government of Canada Communications Security Establishment document "ITSG-33, Annex 3A; Information Technology Security Guidance -- IT Security Risk Management: A Lifecycle Approach, Security Control Catalogue" for definition of the security controls noted in the above Figures 5 and 6.

Schedule A 6 – Security Requirements Traceability Matrix

Shared Services Canada (SSC)

Schedule A 6 – Security Requirements Traceability Matrix

Table of Contents

List of Tables

Schedule A 6 – Security Requirements Traceability Matrix

1.0 Enterprise Service Desk (ESD) Security Requirements Traceability Matrix

Table 52: EDS Security Requirements Traceability Matrix

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the access control policy and associated access controls. (B) The Contractor reviews and updates the current access control policy and associated procedures at least once a year.	(A) (B) frequency [at a frequency no longer than annually]									X	
2	AC-2	ACCOUNT MANAGEMENT		(B) The Contractor establishes the conditions for group membership. There is a documented process for the request, review, and approval for submitting access to the systems.			X	X	X	X				X	
3	AC-2	ACCOUNT MANAGEMENT		(D) The Contractor requires appropriate approvals for requests to establish accounts.			X	X	X	X				X	
4	AC-2	ACCOUNT MANAGEMENT		(E) The Contractor establishes the process for activating, modifying, disabling, and removing accounts.			X	X	X	X				X	
5	AC-2	ACCOUNT MANAGEMENT		(G) The Contractor notifies managers when accounts are no longer required and when users are terminated, transferred, or continued use, or need-to-know changes.			X	X	X	X				X	
6	AC-2	ACCOUNT MANAGEMENT		(J) The Contractor reviews accounts for compliance with account management requirements at least quarterly.			X	X	X	X				X	
7	AC-2	ACCOUNT MANAGEMENT	(5)	The Contractor requires that users log out at the end of the working day and/or if the inactivity is longer than 30 minutes, determines normal time-of-day and duration usage for system or application accounts; monitors for atypical usage of system or application accounts; and reports atypical usage to designated organizational officials.			X	X	X	X				X	
8	AC-2	ACCOUNT MANAGEMENT	(7)	• (a) The Contractor establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; • (b) The Contractor monitors privileged role assignments; and • (c) The Contractor disables, adjusts, or removes access when privileged role assignments are no longer appropriate.			X	X	X	X				X	
9	AC-3	ACCESS ENFORCEMENT	(7)	The Contractor enforces a role-based access control policy over defined subjects and objects and controls access based upon defined roles and users authorized to assume such roles.				X				X		X	
10	AC-4	INFORMATION FLOW ENFORCEMENT		(A) The Contractor enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.			X	X	X	X					
11	AC-6	LEAST PRIVILEGE		(A) The Contractor employs the principle of least privilege, allowing only authorized accesses for user or processes acting on behalf of users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.				X							

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
12	AC-6	LEAST PRIVILEGE	(5)	The Contractor restricts privileged accounts on the information system to defined personnel or roles.				X							
13	AC-6	LEAST PRIVILEGE	(7)	The Contractor: • a) reviews the privileges assigned to defined roles or classes of users least once a year to validate the need for such privileges; and • (b) re-assigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.	(A) (B) frequency [at a frequency no longer than annually]									X	
14	AC-7	UNSUCCESSFUL LOGIN ATTEMPTS		(A) The Contractor enforces a limit of five (5) consecutive invalid logon attempts by a user during a five minute time period. (B) The Contractor automatically locks the account/node for a defined time period; locks the account/node until released by an administrator; delays next logon prompt according to a defined period of time when the maximum number of unsuccessful attempts is exceeded.				X							
15	AC-8	SYSTEM USE NOTIFICATION		(A) The Contractor displays to user system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the TBS Policy on Service and Digital. (B) The Contractor retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.				X							
16	AC-11	SESSION LOCK		(A) The Contractor prevents further access to the system by initiating a session lock after sixty (60) minutes of inactivity or upon receiving a request from a user. (B) The Contractor retains the session lock until the user re-establishes access using established identification and authentication procedures.				X							
17	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. (B) The Contractor reviews and updates the current security awareness and training policy and associated procedures at least once a year.										X	
18	AT-2	SECURITY AWARENESS		(A) The Contractor provides basic security awareness training to all information system users as part of initial training for new users, when required by system changes, and at a fixed interval thereafter.		X								X	
19	AT-3	SECURITY TRAINING		(A) The Contractor provides role-based security-related training before authorizing access to the system or performing assigned duties; when required by system changes; and when a new vulnerability emerges.										X	
20	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. (B) The Contractor reviews and updates the current audit and accountability policy and related procedures at least once a year.	(A) (B) frequency [at a frequency no longer than annually]									X	
21	CM-2	BASELINE CONFIGURATION		(A) The Contractor develops, documents, and maintains under configuration control a current baseline configuration of the system.				X						X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
22	CM-2	BASELINE CONFIGURATION	(2)	The Contractor employs automated mechanisms to maintain an up-to-date, complete accurate and readily available baseline configuration of the system.				X						X	
23	CM-3	CONFIGURATION CHANGE CONTROL		(B) The Contractor approves configuration-controlled changes to the system with explicit consideration for security impact analyses.				X						X	
24	CM-3	CONFIGURATION CHANGE CONTROL		(C) The Contractor documents approved configuration-controlled changes to the system.				X						X	
25	CM-3	CONFIGURATION CHANGE CONTROL	(3)	The Contractor employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.				X						X	
26	CM-6	CONFIGURATION SETTINGS		(A) The Contractor establishes and documents configuration settings for information technology products employed within the information system usage organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements. (B) The Contractor implements the configuration settings. (C) The Contractor identifies, documents, and approves any deviations from established configuration settings for system components based on operational requirements. (D) The Contractor monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.				X						X	
27	CM-6	CONFIGURATION SETTINGS	(1)	The Contractor employs automated mechanisms to centrally manage, apply, and verify configuration settings for system components.				X						X	
28	CM-6	CONFIGURATION SETTINGS	(2)	The Contractor employs security safeguards to respond to unauthorized changes to organization-defined configuration settings.				X						X	
29	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY		(A) The Contractor develops, documents, and maintains an inventory of information system components that accurately reflects the current information system.			X	X	X	X		X		X	
30	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY		(E) The Contractor develops, documents, and maintains an inventory of information system components that is available for review and audit by designated officials.			X	X	X	X		X		X	
31	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. (B) The Contractor reviews and updates the current contingency planning policy and associated procedures at least once a year. (AA) The Contractor develops an audit cycle for the contingency plan program as the basis of regular reporting to SSC.	(C) frequency [at a frequency no longer than annually]									X	
32	CP-2	CONTINGENCY PLAN		(A) The Contractor develops a contingency plan for the information system that: • (a) Identifies essential missions and business functions and associated contingency requirements; • (b) Provides recovery objectives, restoration priorities, and metrics; • (c) Addresses contingency roles, responsibilities, and assigned individuals with contact information; • (d) Addresses maintaining essential missions and business functions despite an										X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				information system disruption, compromise, or failure; • (e) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and • (f) Is reviewed and approved by defined personnel or roles. (B) The Contractor distributes copies of the contingency plan to defined key contingency personnel identified by name and/or by role and organizational elements. (C) The Contractor coordinates contingency planning activities with incident handling activities. (D) The Contractor reviews the contingency plan for the information system defined frequency. (E) The Contractor updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. (F) The Contractor communicates contingency plan changes to defined key contingency personnel identified by name and/or by role and organizational elements. (G) The Contractor protects the contingency plan from unauthorized disclosure and modification.										
33	CP-2	CONTINGENCY PLAN	(2)	The Contractor conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.										X	
34	CP-2	CONTINGENCY PLAN	(3)	The Contractor plans for the resumption of essential missions and business functions as outlined in section 2.9 of the statement of work of contingency plan activation.										X	
35	CP-2	CONTINGENCY PLAN	(4)	The Contractor plans for the resumption of all missions and business functions as outlined in section 2.9 of the statement of work of contingency plan activation.										X	
36	CP-2	CONTINGENCY PLAN	(5)	The Contractor plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.										X	
37	CP-2	CONTINGENCY PLAN	(6)	The Contractor plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites.										X	
38	CP-2	CONTINGENCY PLAN	(7)	The Contractor coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.										X	
39	CP-2	CONTINGENCY PLAN	(8)	The Contractor identifies critical information system assets supporting essential missions and business functions.			X	X	X	X		X		X	
40	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES		(A) The Contractor tests the contingency plan for the information system as outlined in section 2.9 of the statement of work using defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan. (B) The Contractor reviews the contingency plan test results. (C) The Contractor initiates corrective actions, if needed.			X	X	X	X		X		X	
41	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	(1)	The Contractor coordinates contingency plan testing with organizational elements responsible for related plans.			X	X	X	X		X		X	
42	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	(2)	• (a) The Contractor tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources; and • (b) The Contractor tests the contingency plan at the alternate processing site to evaluate the capabilities of the alternate processing site to support contingency operations.			X	X	X	X		X		X	
43	CP-6	ALTERNATE STORAGE SITE		(A) The Contractor establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.											X

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				(B) The Contractor ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.											
44	CP-6	ALTERNATE STORAGE SITE	(1)	The Contractor identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.											X
45	CP-6	ALTERNATE STORAGE SITE	(2)	The Contractor configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.											X
46	CP-7	ALTERNATE PROCESSING SITE	(1)	The Contractor identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.											X
47	CP-7	ALTERNATE PROCESSING SITE	(4)	The Contractor prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.											X
48	CP-8	TELECOMMUNICATIONS SERVICES	(3)	The Contractor obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.								X			
49	CP-9	INFORMATION SYSTEM BACKUP		(A) The Contractor conducts backups of user-level information contained in the information system defined frequency consistent with recovery time and recovery point objectives. (B) The Contractor conducts backups of system-level information contained in the information system defined frequency consistent with recovery time and recovery point objectives. (C) The Contractor conducts backups of information system documentation including security-related documentation defined frequency consistent with recovery time and recovery point objectives. (D) The Contractor protects the confidentiality, integrity, and availability of backup information at storage locations. (AA) The Contractor determines retention periods for essential business information and archived backups.				X							
50	CP-9	INFORMATION SYSTEM BACKUP	(1)	The Contractor tests backup information defined frequency to verify media reliability and information integrity.				X							
51	CP-9	INFORMATION SYSTEM BACKUP	(2)	The Contractor uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.				X							
52	CP-9	INFORMATION SYSTEM BACKUP	(5)	The Contractor transfers information system backup information to the alternate storage site defined time period and transfer rate consistent with the recovery time and recovery point objectives.				X							
53	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. (B) The Contractor reviews and updates the current identification and authentication policy and associated procedures at least once a year.	(A) (B) frequency [at a frequency no longer than annually]										X	
54	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES		(A) The Contractor develops, disseminates, and reviews/updates at least once a year a formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The Contractor develops, disseminates, and reviews/updates at least once a year formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. (AA) The Contractor's incident response policy and procedures facilitate the incorporation of heightened levels of readiness during emergency and heightened IT	(A) (B) frequency [at a frequency no longer than annually]										X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				threat situations in accordance with the GC Directive on Security Management. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32613											
55	IR-4	INCIDENT HANDLING		(A) The Contractor implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. (B) The Contractor coordinates incident handling activities with contingency planning activities. (C) The Contractor incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	(C) frequency [monthly]			X			X			X	X
56	IR-4	INCIDENT HANDLING	(3)	The Contractor identifies organization-defined classes of incidents and organization-defined actions to take in response to classes of incidents to ensure continuation of organizational missions and business functions.				X			X			X	X
57	IR-4	INCIDENT HANDLING	(4)	The Contractor correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.				X			X			X	X
58	IR-6	INCIDENT REPORTING		(A) The Contractor requires personnel to report suspected security incidents the organization's incident response capability within organization-defined time period. (B) The Contractor reports security incident information to organization-defined authorities.	(B) frequency [at a frequency no longer than monthly]			X			X			X	X
59	IR-6	INCIDENT REPORTING	(2)	The Contractor reports information system vulnerabilities associated with reported security incidents to organization-defined personnel or roles.				X			X			X	X
60	IR-8	INCIDENT RESPONSE PLAN		(A) The Contractor develops an incident response plan that: • (a) Provides a roadmap for implementing its incident response capability; • (b) Describes the structure and organization of the incident response capability; • (c) Provides a high-level approach for how the incident response capability fits into the overall organization; • (d) Meets the unique requirements of the Contractor, which relate to mission, size, structure, and functions; • (e) Defines reportable incidents; • (f) Provides metrics for measuring the incident response capability within the organization; • (g) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and • (h) Is reviewed and approved by organization-defined personnel or roles. (B) The Contractor distributes copies of the incident response plan to organization-defined personnel identified by name and/or by role. (C) The Contractor reviews the incident response plan at least once a year. (D) The Contractor updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. (E) The Contractor communicates incident response plan changes to organization-defined incident response personnel identified by name and/or by role) identified. (F) The Contractor protects the incident response plan from unauthorized disclosure and modification.										X	
61	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the media protection policy and	(A) (B) frequency [at a frequency no longer than annually]									X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				associated media protection controls. (B) The Contractor reviews and updates the current media protection policy and associated procedures at least once a year.											
62	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. (B) The Contractor reviews and updates the current physical and environmental protection policy and associated procedures at least once a year.	(A) (B) frequency [at least annually]									X	
63	PE-2	PHYSICAL ACCESS AUTHORIZATIONS		(A) The Contractor develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides. (B) The Contractor issues authorization credentials for facility access. (C) The Contractor reviews the access list detailing authorized facility access by individuals at least once a year. (D) The Contractor removes individuals from the facility access list when access is no longer required.	(A) (B) frequency [at a frequency no longer than annually]										X
64	PE-2	PHYSICAL ACCESS AUTHORIZATIONS	(100)	The Contractor issues an identification card to all personnel, which as a minimum includes the name of the Contractor, the bearer's name and photo, a unique card number and an expiry date.	(A) (B) frequency [at a frequency no longer than annually]										X
65	PE-3	PHYSICAL ACCESS CONTROL		(A) The Contractor enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by: • (a) Verifying individual access authorizations before granting access to the facility; and • (b) Controlling ingress/egress to the facility using organization-defined physical access control systems/devices and guards. (B) The Contractor maintains physical access audit logs for organization-defined entry/exit points. (C) The Contractor provides organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible. (D) The Contractor escorts visitors and monitors visitor activity organization-defined circumstances requiring visitor escorts and monitoring. (E) The Contractor secures keys, combinations, and other physical access devices. (F) The Contractor inventories organization-defined physical access devices every at least once a year. (G) The Contractor changes combinations and keys at least once a year and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	(F) Inventories of physical devices annually (G) Changes combinations and keys when keys are lost, combinations are compromised or individuals are transferred or terminated										X
66	PE-6	MONITORING PHYSICAL ACCESS		(A) The Contractor monitors physical access to the facility where the information system resides to detect and respond to physical security incidents. (B) The Contractor reviews physical access logs at least once a year and upon occurrence of organization-defined events or potential indications of events. (C) The Contractor coordinates results of reviews and investigations wit organization's incident response capability.											X
67	PE-6	MONITORING PHYSICAL ACCESS	(1)	The Contractor monitors physical intrusion alarms and surveillance equipment.											X

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
68	PE-8	ACCESS RECORDS		(A) The Contractor maintains visitor access records to the facility where the information system resides for organization-defined time period; and (B) The Contractor reviews visitor access records at least once a year.											X
69	PL-1	SECURITY PLANNING POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the security planning policy and associated security planning controls. (B) The Contractor reviews and updates the current security planning policy and associated procedures at least once a year.										X	
70	PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. (B) The Contractor reviews and updates the current personnel security policy and associated procedures at least once a year.		X								X	
71	PS-3	PERSONNEL SCREENING		(A) The Contractor screens individuals prior to authorizing access to the information system in accordance with the TBS Standard on Security Screening. (B) The Contractor rescreens individuals according to defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening.		X									
72	PS-3	PERSONNEL SCREENING	(1)	The Contractor ensures that individuals accessing an information system processing, storing, or transmitting types of Protected information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access prior to gaining access to the system and at least once a year.		X									
73	PS-3	PERSONNEL SCREENING	(2)	The Contractor ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: • (a) Have valid access authorizations that are demonstrated by assigned official government duties; and • (b) Satisfies organization-defined additional personnel screening criteria.		X									
74	PS-4	PERSONNEL TERMINATION		(A) The Contractor, upon termination of individual employment disables information system access within one day. (B) The Contractor, upon termination of individual employment terminates/revokes any authenticators/credentials associated with the individual. (C) The Contractor, upon termination of individual employment conducts exit interviews that include a discussion of information security topics. (D) The Contractor, upon termination of individual employment retrieves all security-related organizational information system-related property. (E) The Contractor, upon termination of individual employment retains access to organizational information and information systems formerly controlled by terminated individual. (F) The Contractor, upon termination of individual employment notifies defined personnel or roles within one day.		X									
75	RA-1	RISK ASSESSMENT		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A risk assessment policy that addresses purpose, scope, roles, responsibilities,										X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
		POLICY AND PROCEDURES		management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. (B) The Contractor reviews and updates the current risk assessment policy and associated procedures at least once a year.											
76	RA-3	RISK ASSESSMENT		(A) The Contractor conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. (B) The Contractor documents risk assessment results in a risk assessment report. (C) The Contractor reviews risk assessment results least once year. (D) The Contractor disseminates risk assessment results to defined personnel or roles. (E) The Contractor updates the risk assessment at least once a year or whenever there are significant changes to the information system or environment of operation including the identification of new threats and vulnerabilities, or other conditions that may impact the security state of the system.				X	X			X			
77	RA-5	VULNERABILITY SCANNING		(A) The Contractor scans for vulnerabilities in the information system at least once a year and when new vulnerabilities potentially affecting the system are identified and reported. (B) The Contractor employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process: • (a) Enumerating platforms, software flaws, and improper configurations; • (b) Formatting checklists and test procedures; and • (c) Measuring vulnerability impact. (C) The Contractor analyzes vulnerability scan reports and results from security control assessments. (D) The Contractor remediates legitimate vulnerabilities within two weeks in accordance with an organizational assessment of risk. (E) The Contractor shares information obtained from the vulnerability scanning process and security control assessments with defined personnel or roles.									X	
78	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. (B) The Contractor reviews and updates the current system and services acquisition policy and associated procedures at least once a year.										X	
79	SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. (B) The Contractor reviews and updates the current system and communications protection policy and associated procedures at least once a year.										X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
80	SC-7	BOUNDARY PROTECTION		(A) The Contractor monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. (B) The Contractor implements sub-networks for publicly accessible system components that are physically and logically separated from internal organizational networks. (C) The Contractor connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.								X			
81	SC-7	BOUNDARY PROTECTION	(3)	The Contractor limits the number of external network connections to the information system.								X	X		
82	SC-7	BOUNDARY PROTECTION	(4)	• (a) The Contractor implements a managed interface for each external telecommunication service; • (b) The Contractor establishes a traffic flow policy for each managed interface; • (c) The Contractor protects the confidentiality and integrity of the information being transmitted across each interface; • (d) The Contractor documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and • (e) The Contractor reviews exceptions to the traffic flow policy and removes exceptions that are no longer supported by an explicit mission/business need.								X	X		
83	SC-8	TRANSMISSION INTEGRITY	(1)	The Contractor implements cryptographic mechanisms to prevent unauthorized disclosure of information; detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards. The cryptography must be compliant with the requirements of control SC-13.				X							
84	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	(2)	The Contractor maintains the confidentiality and/or integrity of information during preparation for transmission and during reception.				X							
85	SC-13	USE OF CRYPTOGRAPHY		(A) The Contractor implements cryptographic protections using cryptographic systems that comply with applicable GC legislation and TBS policies, directives and standards.				X							
86	SC-23	SESSION AUTHENTICITY		(A) The Contractor protects the authenticity of communications sessions.								X			
87	SC-23	SESSION AUTHENTICITY	(3)	The Contractor generates a unique session identifier for each session with organization-defined randomness requirements and recognizes only session identifiers that are system-generated.								X			
88	SC-28	PROTECTION OF INFORMATION AT REST		(A) The Contractor protects the confidentiality and integrity of organization-defined information at rest.				X							
89	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. (B) The Contractor reviews and updates the current system and information integrity policy and associated procedures at least once a year.										X	
90	SI-2	FLAW REMEDIATION		(A) The Contractor identifies, reports, and corrects system flaws.			X	X	X	X	X	X	X	X	X
91	SI-2	FLAW REMEDIATION		(B) The Contractor tests software updates related to flaw remediation for effectiveness and potential side effects on systems before installation.				X							

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C1.3	C.4	C.5	C.6	C.8	D.1 & D.2	D.3	Policies / Plans	Delivery Location
92	SI-2	FLAW REMEDIATION		(C) The Contractor installs security-relevant software and firmware updates within fourteen (14) federal government working days of the release of the updates and within forty-eight (48) hours for critical updates.				X							
93	SI-12	INFORMATION OUTPUT HANDLING AND RETENTION		(A) The Contractor handles and retains both information within and output from the system in accordance with applicable GC legislation and TBS policies, directives and standards, and operational requirements.				X							X

2.0 End User Service Desk (EUSD) Security Requirements Traceability Matrix

Table 53: EUSD Security Requirements Traceability Matrix

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the access control policy and associated access controls. (B) The Contractor reviews and updates the current access control policy and associated procedures at least once a year.	(A) (B) frequency [at a frequency no longer than annually]									X	
2	AC-2	ACCOUNT MANAGEMENT		(B) The Contractor establishes the conditions for group membership. There is a documented process for the request, review, and approval for submitting access to the systems.			X	X	X	X				X	
3	AC-2	ACCOUNT MANAGEMENT		(D) The Contractor requires appropriate approvals for requests to establish accounts.			X	X	X	X				X	
4	AC-2	ACCOUNT MANAGEMENT		(E) The Contractor establishes the process for activating, modifying, disabling, and removing accounts.			X	X	X	X				X	
5	AC-2	ACCOUNT MANAGEMENT		(G) The Contractor notifies managers when accounts are no longer required and when users are terminated, transferred, or continued use, or need-to-know changes.			X	X	X	X				X	
6	AC-2	ACCOUNT MANAGEMENT		(J) The Contractor reviews accounts for compliance with account management requirements at least quarterly.			X	X	X	X				X	
7	AC-2	ACCOUNT MANAGEMENT	(5)	The Contractor requires that users log out at the end of the working day and/or if the inactivity is longer than 30 minutes, determines normal time-of-day and duration usage for system or application accounts; monitors for atypical usage of system or application accounts; and reports atypical usage to designated organizational officials.			X	X	X	X				X	
8	AC-2	ACCOUNT MANAGEMENT	(7)	• (a) The Contractor establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; • (b) The Contractor monitors privileged role assignments; and • (c) The Contractor disables, adjusts, or removes access when privileged role assignments are no longer appropriate.			X	X	X	X				X	
9	AC-3	ACCESS ENFORCEMENT	(7)	The Contractor enforces a role-based access control policy over defined subjects and objects and controls access based upon defined roles and users authorized to assume such roles.				X				X		X	
10	AC-4	INFORMATION FLOW ENFORCEMENT		(A) The Contractor enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.			X	X	X	X					
11	AC-6	LEAST PRIVILEGE		(A) The Contractor employs the principle of least privilege, allowing only authorized accesses for user or processes acting on behalf of users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.				X							
12	AC-6	LEAST PRIVILEGE	(5)	The Contractor restricts privileged accounts on the information system to defined personnel or roles.				X							
13	AC-6	LEAST PRIVILEGE	(7)	The Contractor:	(A) (B) frequency [at									X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				• a) reviews the privileges assigned to defined roles or classes of users least once a year to validate the need for such privileges; and • (b) re-assigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.	a frequency no longer than annually]										
14	AC-7	UNSUCCESSFUL LOGIN ATTEMPTS		(A) The Contractor enforces a limit of five (5) consecutive invalid logon attempts by a user during a five minute time period. (B) The Contractor automatically locks the account/node for a defined time period; locks the account/node until released by an administrator; delays next logon prompt according to a defined period of time when the maximum number of unsuccessful attempts is exceeded.				X							
15	AC-8	SYSTEM USE NOTIFICATION		(A) The Contractor displays to user system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with the TBS Policy on Service and Digital. (B) The Contractor retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.				X							
16	AC-11	SESSION LOCK		(A) The Contractor prevents further access to the system by initiating a session lock after sixty (60) minutes of inactivity or upon receiving a request from a user. (B) The Contractor retains the session lock until the user re-establishes access using established identification and authentication procedures.				X							
17	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. (B) The Contractor reviews and updates the current security awareness and training policy and associated procedures at least once a year.										X	
18	AT-2	SECURITY AWARENESS		(A) The Contractor provides basic security awareness training to all information system users as part of initial training for new users, when required by system changes, and at a fixed interval thereafter.		X								X	
19	AT-3	SECURITY TRAINING		(A) The Contractor provides role-based security-related training before authorizing access to the system or performing assigned duties; when required by system changes; and when a new vulnerability emerges.										X	
20	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. (B) The Contractor reviews and updates the current audit and accountability policy and related procedures at least once a year.	(A) (B) frequency [at a frequency no longer than annually]									X	
21	CM-2	BASELINE CONFIGURATION		(A) The Contractor develops, documents, and maintains under configuration control a current baseline configuration of the system.				X						X	
22	CM-2	BASELINE CONFIGURATION	(2)	The Contractor employs automated mechanisms to maintain an up-to-date, complete accurate and readily available baseline configuration of the system.				X						X	
23	CM-3	CONFIGURATION CHANGE CONTROL		(B) The Contractor approves configuration-controlled changes to the system with explicit consideration for security impact analyses.				X						X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
24	CM-3	CONFIGURATION CHANGE CONTROL		(C) The Contractor documents approved configuration-controlled changes to the system.				X						X	
25	CM-3	CONFIGURATION CHANGE CONTROL	(3)	The Contractor employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.				X						X	
26	CM-6	CONFIGURATION SETTINGS		(A) The Contractor establishes and documents configuration settings for information technology products employed within the information system usage organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements. (B) The Contractor implements the configuration settings. (C) The Contractor identifies, documents, and approves any deviations from established configuration settings for system components based on operational requirements. (D) The Contractor monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.				X						X	
27	CM-6	CONFIGURATION SETTINGS	(1)	The Contractor employs automated mechanisms to centrally manage, apply, and verify configuration settings for system components.				X						X	
28	CM-6	CONFIGURATION SETTINGS	(2)	The Contractor employs security safeguards to respond to unauthorized changes to organization-defined configuration settings.				X						X	
29	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY		(A) The Contractor develops, documents, and maintains an inventory of information system components that accurately reflects the current information system.			X	X	X	X		X		X	
30	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY		(E) The Contractor develops, documents, and maintains an inventory of information system components that is available for review and audit by designated officials.			X	X	X	X		X		X	
31	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. (B) The Contractor reviews and updates the current contingency planning policy and associated procedures at least once a year. (AA) The Contractor develops an audit cycle for the contingency plan program as the basis of regular reporting to SSC.	(C) frequency [at a frequency no longer than annually]									X	
32	CP-2	CONTINGENCY PLAN		(A) The Contractor develops a contingency plan for the information system that: • (a) Identifies essential missions and business functions and associated contingency requirements; • (b) Provides recovery objectives, restoration priorities, and metrics; • (c) Addresses contingency roles, responsibilities, and assigned individuals with contact information; • (d) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; • (e) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and • (f) Is reviewed and approved by defined personnel or roles. (B) The Contractor distributes copies of the contingency plan to defined key									X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				contingency personnel identified by name and/or by role and organizational elements. (C) The Contractor coordinates contingency planning activities with incident handling activities. (D) The Contractor reviews the contingency plan for the information system defined frequency. (E) The Contractor updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. (F) The Contractor communicates contingency plan changes to defined key contingency personnel identified by name and/or by role and organizational elements. (G) The Contractor protects the contingency plan from unauthorized disclosure and modification.										
33	CP-2	CONTINGENCY PLAN	(2)	The Contractor conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.										X	
34	CP-2	CONTINGENCY PLAN	(3)	The Contractor plans for the resumption of essential missions and business functions as outlined in section 2.9 of the statement of work of contingency plan activation.										X	
35	CP-2	CONTINGENCY PLAN	(4)	The Contractor plans for the resumption of all missions and business functions as outlined in section 2.9 of the statement of work of contingency plan activation.										X	
36	CP-2	CONTINGENCY PLAN	(5)	The Contractor plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.										X	
37	CP-2	CONTINGENCY PLAN	(6)	The Contractor plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites.										X	
38	CP-2	CONTINGENCY PLAN	(7)	The Contractor coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.										X	
39	CP-2	CONTINGENCY PLAN	(8)	The Contractor identifies critical information system assets supporting essential missions and business functions.			X	X	X	X		X		X	
40	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES		(A) The Contractor tests the contingency plan for the information system as outlined in section 2.9 of the statement of work using defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan. (B) The Contractor reviews the contingency plan test results. (C) The Contractor initiates corrective actions, if needed.			X	X	X	X		X		X	
41	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	(1)	The Contractor coordinates contingency plan testing with organizational elements responsible for related plans.			X	X	X	X		X		X	
42	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	(2)	• (a) The Contractor tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources; and • (b) The Contractor tests the contingency plan at the alternate processing site to evaluate the capabilities of the alternate processing site to support contingency operations.			X	X	X	X		X		X	
43	CP-6	ALTERNATE STORAGE SITE		(A) The Contractor establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information. (B) The Contractor ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.											X
44	CP-6	ALTERNATE STORAGE SITE	(1)	The Contractor identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.											X

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
45	CP-6	ALTERNATE STORAGE SITE	(2)	The Contractor configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.											X
46	CP-7	ALTERNATE PROCESSING SITE	(1)	The Contractor identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.											X
47	CP-7	ALTERNATE PROCESSING SITE	(4)	The Contractor prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.											X
48	CP-8	TELECOMMUNICATIONS SERVICES	(3)	The Contractor obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.								X			
49	CP-9	INFORMATION SYSTEM BACKUP		(A) The Contractor conducts backups of user-level information contained in the information system defined frequency consistent with recovery time and recovery point objectives. (B) The Contractor conducts backups of system-level information contained in the information system defined frequency consistent with recovery time and recovery point objectives. (C) The Contractor conducts backups of information system documentation including security-related documentation defined frequency consistent with recovery time and recovery point objectives. (D) The Contractor protects the confidentiality, integrity, and availability of backup information at storage locations. (AA) The Contractor determines retention periods for essential business information and archived backups.				X							
50	CP-9	INFORMATION SYSTEM BACKUP	(1)	The Contractor tests backup information defined frequency to verify media reliability and information integrity.				X							
51	CP-9	INFORMATION SYSTEM BACKUP	(2)	The Contractor uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.				X							
52	CP-9	INFORMATION SYSTEM BACKUP	(5)	The Contractor transfers information system backup information to the alternate storage site defined time period and transfer rate consistent with the recovery time and recovery point objectives.				X							
53	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. (B) The Contractor reviews and updates the current identification and authentication policy and associated procedures at least once a year.	(A) (B) frequency [at a frequency no longer than annually]									X	
54	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES		(A) The Contractor develops, disseminates, and reviews/updates at least once a year a formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. (B) The Contractor develops, disseminates, and reviews/updates at least once a year formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. (AA) The Contractor's incident response policy and procedures facilitate the incorporation of heightened levels of readiness during emergency and heightened IT threat situations in accordance with the GC Directive on Security Management. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32613	(A) (B) frequency [at a frequency no longer than annually]									X	
55	IR-4	INCIDENT HANDLING		(A) The Contractor implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	(C) frequency [monthly			X			X			X	X

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				(B) The Contractor coordinates incident handling activities with contingency planning activities. (C) The Contractor incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.												
56	IR-4	INCIDENT HANDLING	(3)	The Contractor identifies organization-defined classes of incidents and organization-defined actions to take in response to classes of incidents to ensure continuation of organizational missions and business functions.				X			X			X	X
57	IR-4	INCIDENT HANDLING	(4)	The Contractor correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.				X			X			X	X
58	IR-6	INCIDENT REPORTING		(A) The Contractor requires personnel to report suspected security incidents the organization's incident response capability within organization-defined time period. (B) The Contractor reports security incident information to organization-defined authorities.	(B) frequency [at a frequency no longer than monthly]			X			X			X	X
59	IR-6	INCIDENT REPORTING	(2)	The Contractor reports information system vulnerabilities associated with reported security incidents to organization-defined personnel or roles.				X			X			X	X
60	IR-8	INCIDENT RESPONSE PLAN		(A) The Contractor develops an incident response plan that: • (a) Provides a roadmap for implementing its incident response capability; • (b) Describes the structure and organization of the incident response capability; • (c) Provides a high-level approach for how the incident response capability fits into the overall organization; • (d) Meets the unique requirements of the Contractor, which relate to mission, size, structure, and functions; • (e) Defines reportable incidents; • (f) Provides metrics for measuring the incident response capability within the organization; • (g) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and • (h) Is reviewed and approved by organization-defined personnel or roles. (B) The Contractor distributes copies of the incident response plan to organization-defined personnel identified by name and/or by role. (C) The Contractor reviews the incident response plan at least once a year. (D) The Contractor updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. (E) The Contractor communicates incident response plan changes to organization-defined incident response personnel identified by name and/or by role) identified. (F) The Contractor protects the incident response plan from unauthorized disclosure and modification.										X	
61	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the media protection policy and associated media protection controls. (B) The Contractor reviews and updates the current media protection policy and associated procedures at least once a year.	(A) (B) frequency [at a frequency no longer than annually]									X	
62	PE-1	PHYSICAL AND ENVIRONMENTAL		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year:	(A) (B) frequency [at									X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
		PROTECTION POLICY AND PROCEDURES		• (a) A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. (B) The Contractor reviews and updates the current physical and environmental protection policy and associated procedures at least once a year.	least annually]										
63	PE-2	PHYSICAL ACCESS AUTHORIZATIONS		(A) The Contractor develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides. (B) The Contractor issues authorization credentials for facility access. (C) The Contractor reviews the access list detailing authorized facility access by individuals at least once a year. (D) The Contractor removes individuals from the facility access list when access is no longer required.	(A) (B) frequency [at a frequency no longer than annually]										X
64	PE-2	PHYSICAL ACCESS AUTHORIZATIONS	(100)	The Contractor issues an identification card to all personnel, which as a minimum includes the name of the Contractor, the bearer's name and photo, a unique card number and an expiry date.	(A) (B) frequency [at a frequency no longer than annually]										X
65	PE-3	PHYSICAL ACCESS CONTROL		(A) The Contractor enforces physical access authorizations at organization-defined entry/exit points to the facility where the information system resides by: • (a) Verifying individual access authorizations before granting access to the facility; and • (b) Controlling ingress/egress to the facility using organization-defined physical access control systems/devices and guards. (B) The Contractor maintains physical access audit logs for organization-defined entry/exit points. (C) The Contractor provides organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible. (D) The Contractor escorts visitors and monitors visitor activity organization-defined circumstances requiring visitor escorts and monitoring. (E) The Contractor secures keys, combinations, and other physical access devices. (F) The Contractor inventories organization-defined physical access devices every at least once a year. (G) The Contractor changes combinations and keys at least once a year and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	(F) Inventories of physical devices annually (G) Changes combinations and keys when keys are lost, combinations are compromised or individuals are transferred or terminated										X
66	PE-6	MONITORING PHYSICAL ACCESS		(A) The Contractor monitors physical access to the facility where the information system resides to detect and respond to physical security incidents. (B) The Contractor reviews physical access logs at least once a year and upon occurrence of organization-defined events or potential indications of events. (C) The Contractor coordinates results of reviews and investigations wit organization's incident response capability.											X
67	PE-6	MONITORING PHYSICAL ACCESS	(1)	The Contractor monitors physical intrusion alarms and surveillance equipment.											X
68	PE-8	ACCESS RECORDS		(A) The Contractor maintains visitor access records to the facility where the information system resides for organization-defined time period; and (B) The Contractor reviews visitor access records at least once a year.											X
69	PL-1	SECURITY PLANNING POLICY		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year:										X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
		AND PROCEDURES		• (a) A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the security planning policy and associated security planning controls. (B) The Contractor reviews and updates the current security planning policy and associated procedures at least once a year.											
70	PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. (B) The Contractor reviews and updates the current personnel security policy and associated procedures at least once a year.		X								X	
71	PS-3	PERSONNEL SCREENING		(A) The Contractor screens individuals prior to authorizing access to the information system in accordance with the TBS Standard on Security Screening. (B) The Contractor rescreens individuals according to defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening.		X									
72	PS-3	PERSONNEL SCREENING	(1)	The Contractor ensures that individuals accessing an information system processing, storing, or transmitting types of Protected information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access prior to gaining access to the system and at least once a year.		X									
73	PS-3	PERSONNEL SCREENING	(2)	The Contractor ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: • (a) Have valid access authorizations that are demonstrated by assigned official government duties; and • (b) Satisfies organization-defined additional personnel screening criteria.		X									
74	PS-4	PERSONNEL TERMINATION		(A) The Contractor, upon termination of individual employment disables information system access within one day. (B) The Contractor, upon termination of individual employment terminates/revokes any authenticators/credentials associated with the individual. (C) The Contractor, upon termination of individual employment conducts exit interviews that include a discussion of information security topics. (D) The Contractor, upon termination of individual employment retrieves all security-related organizational information system-related property. (E) The Contractor, upon termination of individual employment retains access to organizational information and information systems formerly controlled by terminated individual. (F) The Contractor, upon termination of individual employment notifies defined personnel or roles within one day.		X									
75	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.										X	

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				(B) The Contractor reviews and updates the current risk assessment policy and associated procedures at least once a year.											
76	RA-3	RISK ASSESSMENT		(A) The Contractor conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. (B) The Contractor documents risk assessment results in a risk assessment report. (C) The Contractor reviews risk assessment results least once year. (D) The Contractor disseminates risk assessment results to defined personnel or roles. (E) The Contractor updates the risk assessment at least once a year or whenever there are significant changes to the information system or environment of operation including the identification of new threats and vulnerabilities, or other conditions that may impact the security state of the system.				X	X			X			
77	RA-5	VULNERABILITY SCANNING		(A) The Contractor scans for vulnerabilities in the information system at least once a year and when new vulnerabilities potentially affecting the system are identified and reported. (B) The Contractor employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process: • (a) Enumerating platforms, software flaws, and improper configurations; • (b) Formatting checklists and test procedures; and • (c) Measuring vulnerability impact. (C) The Contractor analyzes vulnerability scan reports and results from security control assessments. (D) The Contractor remediates legitimate vulnerabilities within two weeks in accordance with an organizational assessment of risk. (E) The Contractor shares information obtained from the vulnerability scanning process and security control assessments with defined personnel or roles.									X	
78	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. (B) The Contractor reviews and updates the current system and services acquisition policy and associated procedures at least once a year.										X	
79	SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. (B) The Contractor reviews and updates the current system and communications protection policy and associated procedures at least once a year.										X	
80	SC-7	BOUNDARY PROTECTION		(A) The Contractor monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. (B) The Contractor implements sub-networks for publicly accessible system components that are physically and logically separated from internal organizational								X			

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
				networks. (C) The Contractor connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.											
81	SC-7	BOUNDARY PROTECTION	(3)	The Contractor limits the number of external network connections to the information system.								X	X		
82	SC-7	BOUNDARY PROTECTION	(4)	• (a) The Contractor implements a managed interface for each external telecommunication service; • (b) The Contractor establishes a traffic flow policy for each managed interface; • (c) The Contractor protects the confidentiality and integrity of the information being transmitted across each interface; • (d) The Contractor documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and • (e) The Contractor reviews exceptions to the traffic flow policy and removes exceptions that are no longer supported by an explicit mission/business need.								X	X		
83	SC-8	TRANSMISSION INTEGRITY	(1)	The Contractor implements cryptographic mechanisms to prevent unauthorized disclosure of information; detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards. The cryptography must be compliant with the requirements of control SC-13.				X							
84	SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	(2)	The Contractor maintains the confidentiality and/or integrity of information during preparation for transmission and during reception.				X							
85	SC-13	USE OF CRYPTOGRAPHY		(A) The Contractor implements cryptographic protections using cryptographic systems that comply with applicable GC legislation and TBS policies, directives and standards.				X							
86	SC-23	SESSION AUTHENTICITY		(A) The Contractor protects the authenticity of communications sessions.								X			
87	SC-23	SESSION AUTHENTICITY	(3)	The Contractor generates a unique session identifier for each session with organization-defined randomness requirements and recognizes only session identifiers that are system-generated.								X			
88	SC-28	PROTECTION OF INFORMATION AT REST		(A) The Contractor protects the confidentiality and integrity of organization-defined information at rest.				X							
89	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES		(A) The Contractor develops, documents, and disseminates to organization-defined personnel or roles, at least once a year: • (a) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and • (b) Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. (B) The Contractor reviews and updates the current system and information integrity policy and associated procedures at least once a year.										X	
90	SI-2	FLAW REMEDIATION		(A) The Contractor identifies, reports, and corrects system flaws.			X	X	X	X	X	X	X	X	X
91	SI-2	FLAW REMEDIATION		(B) The Contractor tests software updates related to flaw remediation for effectiveness and potential side effects on systems before installation.				X							
92	SI-2	FLAW REMEDIATION		(C) The Contractor installs security-relevant software and firmware updates within fourteen (14) federal government working days of the release of the updates and within forty-eight (48) hours for critical updates.				X							
93	SI-12	INFORMATION OUTPUT		(A) The Contractor handles and retains both information within and output from the system in accordance with applicable GC legislation and TBS policies, directives and standards, and operational requirements.				X							X

#	Control ID	Name	Enhance-ment	Definition	Placeholder Value	A.2	C3.3	C.4	C.5	C.6	C.9	D.1 & D.2	D.3	Policies / Plans	Delivery Location
		HANDLING AND RETENTION													

Schedule A 7 – Glossary; Definition of Key Terms

Shared Services Canada (SSC)

Schedule A 7 – Glossary; Definition of Key Terms

Table of Contents

List of Tables

Schedule A 7 – Glossary; Definition of Key Terms

1.0 Glossary

Table 54: Glossary

Term	Definition
ACD	Automated Call Distributor
ARC	Additional Resource Charge
BCP	Business Continuity Plan
CBAS	Critical Business Applications and Services
CM	Change Management
CI	Configurable Item
CISD/PSPC	Canadian Industrial Security Directorate of Public Services and Procurement Canada
CMDB	Configuration Management Database
COTS	Commercial Off-the-Shelf
CSAT	Customer Satisfaction
CSPS	Canada School of the Public Service
DOS	Document Organization Screening
DR	Disaster Recovery
DS	Designated Sites
DSC	Document Safeguarding Capability
ECD	Enterprise Control Desk
ESD	Enterprise Service Desk
EUD	End User Devices
EUSD	End User Service Desk
FCR	First Contact Resolution
FGWD	Federal Government Working Days
FSC	Facility Security Clearance
GC	Government of Canada
GCNET	Government of Canada Network
GCSX	Government of Canada Service Express
GMD	General Management Documentation
GOP	Government Operations Portfolio
HAW	High Awareness Window
HC	Health Canada
HCCS	Hosted Contact Centre Service
IAM	Identity and Access Management
IM	Information Management

Term	Definition
IMAC	Installs, Moves, Adds, Changes
INFC	Infrastructure Canada
IT	Information Technology
ITIL	Information Technology Information Library
ITSM	Information Technology Service Management
IVR	Interactive Voice Response
KPI	Key Performance Indicator
MIS	Management Information System
MSI	Multi-Sourcing Service Integration
NCR	National Capital Region
NSD	National Service Desk
OLA	Operational-Level Agreement
OSSRO	Office System Service Request Online
PAZ	Public Access Zone
PM	Problem Management
PMIC	Partner Major Incident Coordinator
PSD	Partner Service Desks
PSTN	Public Switched Telephone Network
PZ	Public Zone
PSPC	Public Services and Procurement Canada
P2P	Peer-to-Peer
RCA	Root Cause Analysis
RFC	Request for Change
RRC	Reduce Resource Charge
RZ	Restricted Zone
SDAM	Service Delivery and Management
SDM	Service Delivery Manual
SDRF	Service Desk and Request Fulfilment
SIAM	Service Integration and Management
SLA	Service Level Agreement
SLR	Service Level Requirement
SOP	Standard Operating Procedures
SOW	Statement of Work
SPOC	Single Point of Contact
SQL	Structured Query Language
SRTM	Security Requirement Traceability Matrix
SSC	Shared Services Canada
SSEMD	Safety, Security and Emergency Management Division
SSO	Single Sign-On

Term	Definition
TOTP	Time Based One-Time Password
TBS	Treasury Board Secretariat
TBD	To be Determined
TR&R	Technology Refreshment and Replenishment
UAT	User Acceptance Test
VDI	Virtual Desktop Infrastructure
VoIP	Voice over IP
WAN	Wide Area Network
WBS	Work Breakdown Structure

2.0 Definitions

"Actual Service Volume" means Qualifying Contacts for the Enterprise Service Desk (ESD) and End User Service Desk (EUSD) in a month.

"Additional Service Level Credit" means the Service Level Credit that will apply in addition to the base Service Level Credit for failure to meet the Minimum Service Level in the consecutive months following a Service Level Failure for a given Service Level Category.

"Additional Resource Charges" or "ARCs" means an additional resource charge, as calculated in accordance with this Schedule B 1 – Pricing Provisions.

"Additional Resource Charges Unit Rate" or "ARC Unit Rate" means , with respect to a Base Service to be charged using a Monthly Variable Service Cost, the unit dollar charge rate for certain excess Service Volumes experienced by Shared Services Canada (SSC) during a Measurement Period, as set forth in Section 2.2 of **ANNEX B – BASIS OF PAYMENT**.

"At Risk Amount" means the total amount of Service Level Credits that can be owed by the Contractor in any given month expressed as a percentage of total monthly charges. For the purposes of this Contract, the At Risk Amount is established in **Schedule B 2 – Service Level Requirements**.

"Base Services" means each ongoing, recurring Service provided by the Contractor to SSC pursuant to the Statement of Work as set forth in **ANNEX A – STATEMENT OF WORK**.

"Chat Abandonment Rate" means the proportion of chat contacts abandoned after 60 seconds from entering the chat queue to the total number of chat contacts entering the chat queue and remaining more than 60 seconds.

"Chat Answer Rate" means the proportion of chat contacts answered within the Performance Target of entering the chat queue to the total number of chat contacts answered.

"Contract Term" means the entire period of time during which the Contractor is obliged to perform the Service Desk Services which includes the three (3) year period of the initial contract and the period during which the Contract is extended, if SSC chooses to exercise any options set out in the Contract.

"Contract" means the agreement between SSC and the Contractor for the provision of Service Desk Services during the Contract Term.

"Contractor" means the service provider engaged to provide the Service Desk Services.

"Contractor Personnel" means employees, agents, sub-contractors and management of the Contractor and/or its Partner(s) working at the Contractor Premises.

"Contractor Facilities" means the two distinct Contractor-provided delivery locations accommodating the ESD and EUSD.

"Corrective Action Plan" means the planned actions to be taken by the Contractor in the instance of a Service Level Failure. The Corrective Action Plan represents the Contractor's detailed steps to be taken to prevent recurrence of the Service Level Failure.

"Chronic Service Level Failures" means Service Level Failures in 2 or more consecutive months for the same Service Level Category.

"CSAT Score" means Customer Service Satisfaction Scores obtained through post-contact survey as described in **Schedule B 2 – Service Level Requirements**.

"Customer Satisfaction (CSAT)" means a subjective rating obtained through a combination of post-contact surveys and feedback from random follow-up calls to Service Desk Agents.

"Dead Band" means the percentage variance of Service Volumes above or below the Monthly Baseline Service Volumes, and within which ARCs (Additional Resource Charges) and RRCs (Reduced Resource Charges) are not applicable. This is set at five percent (5%).

"Earn Back Amount" means the amount of service level credits returnable to the Contractor as the result of delivering service at or above the Minimum Service Level for a given Service Level Category in each of the three (3) months immediately following the month in which a Service Level Failure ("Originating Service Level Failure") occurred for that given Service Level Category. See **Schedule B 2 – Service Level Requirements**.

"E-mail Listener" means the custom application which operates as a bridge between partner ESD ITSM Tool(s) and ITSM Tool(s) used by ESD Customers.

"Email Response Rate" means the proportion of email contacts responded by Service Desk Agents within the Performance Target of entering the queue to the total number of email contacts responded by Service Desk Agents.

"End-users" means employees and contractors employed by EUSD Customers. End-users contact the EUSD for desktop environment related issues.

"Enterprise Services" means mandated email, telecommunications, data centre and network services that SSC is responsible for delivering to ESD Customers.

"ESD Customers" means all Partner Departments and Non-Partner Clients.

"ESD ITSM Tool(s)" means the Information Technology Service Management (ITSM) Tool(s) used to create and track reported incidents and service requests for ESD Customers. ITSM Tool(s) used by the ESD are specifically identified in Section 1 of **Schedule B 3 – Financial Responsibility Matrix**.

"ESD Service Desk Agents" means those Service Desk Agents providing Single Point of Contact Services for ESD Customers.

"EUSD Customers" means the five departments for which SSC provides end-user support. EUSD Customers defined in **Schedule A 12 – Customers Supported**.

"EUSD ITSM Tool(s)" means the Information Technology Service Management (ITSM) tool(s) used to create and track reported incidents and service requests for EUSD Customers. ITSM Tool(s) used by the EUSD are specifically identified in Section 2 of **Schedule B 3 – Financial Responsibility Matrix**.

"EUSD Service Desk Agents" means those Service Desk Agents providing Single Point of Contact Services for EUSD Customers.

"Excusable Event" means those events or circumstances outside the reasonable control of the Contractor, including a Force Majeure Event, to the extent excused in accordance with the Contract. For greater clarity, a labour action shall not constitute an excusable event.

"Federal Government Working Days" means Mondays through Fridays inclusive, excluding Federal Statutory Holidays.

"Final Services Commencement Date" means the date at which SSC has approved the service(s) to be deployed, as per Section 3.1.6 of **Schedule A 3 – Transition Services**, Table 46, item 6.19.

"First Contact Resolution" means those reported incidents or service requests that are resolved at initial point of contact with a Service Desk Agent without requiring dispatch, escalation or assignment to another service desk or resolver group.

"Force Majeure" means any acts or omissions of any civil or military authority, acts of terrorism, acts of God, fires, strikes or other labor disturbances, equipment failures, fluctuations or non-availability of electrical power, heat, light, air conditioning or telecommunications equipment, or any other similar act, omission or occurrence beyond either the Contractor or SSC reasonable control.

"Fully On-boarded" means those Partner Departments who have transitioned from their legacy ITSM Tool to the ESD ITSM Tool. Fully On-Boarded Partners are identified in Section 1.2 and Section 1.3 of **Schedule A 12 – Customers Supported**.

"**Heightened Awareness Window**" means that during times of emergency and crisis, SSC may invoke the Heightened Awareness Window (HAW) in support of Government of Canada actions. The HAW is enforced to ensure that technical teams respond quickly in the event of an incident (no matter the priority) affecting a particular Service, Application, etc. The HAW is used to ensure technical teams are on call above and beyond normal hours of service. Although the HAW will trigger an immediate response, it is still integrated with the existing Incident Management process. The HAW process is not used to stop Request For Change (RFC) from being implemented.

"Hosted Contact Center Service" means the telephony platform provided by SSC for use by the Contractor in the performance of its obligations to provide Service Desk Services.

"Incident Coordinator" means Government of Canada employees or contractors with responsibility for incident management relating to High, Critical or HAW events.

"Incumbent Contractor" means the service provider currently providing Service Desk Services to SSC.

"Incumbent Contractor Personnel" means employees, agents, sub-contractors and management of the Incumbent Contractor and/or its Partner(s) working at SSC premises.

"Level of Service" means the level of performance achieved by the Contractor for a given Service Level Category in a given month.

"Milestone Deadlines" means the committed timelines for the Contractor to complete the Planned Actions established in the Corrective Action Plan.

"Minimum Service Level" means the minimum Level of Service required for each Service Level Category in order for the Contractor to avoid a Service Level Credit in a given month. Minimum Service Levels are established as Service Level Requirements.

"Monthly Baseline Service Volume"
Means the Monthly Baseline Service Volumes established in Section 2.1.1 of **ANNEX B – BASIS OF PAYMENT**.

"Monthly Variable Service Cost" means the periodic Cost for the volume of each Base Service performed by the Contractor and consumed by SSC in the amount of the Monthly Baseline Service Volume for such Base Service, for a particular month.

"Non-Partner Clients" means those Government of Canada agencies/organizations consuming limited Enterprise Services. Non-partner Clients are specifically identified in **Schedule A – 12 Customer Supported**.

"Non-Partner Service Desks" means the end user Service Desks for Non-Partner Clients.

"Non-Partner Service Desks Agents" means the service desk agents employed by Non-Partner Service Desks.

"Non-Resolvable Contacts" are those incidents/service requests for which the ESD Service Desk Agents and EUSD Service Desk Agents are expected to assign to Service Line Resolver Groups (in the Case of the ESD) or escalate to the ESD (in the case of the EUSD).

"Originating Service Level Failure" means the Service Level Failure giving rise to a Service Level Credit for which the Contractor, may be entitled to receive an Earn Back Amount.

"Out-of-Scope Contacts" means those contacts that inadvertently arrive at the ESD or the EUSD but that should instead have gone to another desk or organization. Out-of-Scope contacts should be re-directed to the appropriate desk or organization through manual or automatic means (i.e. ACD).

"Partner Departments" means those Government of Canada departments that are mandated to consume SSC provided Enterprise Services. Partner Departments are specifically identified in **Schedule A – 12 Customers Supported**.

"Partner Service Desks" means the End User Service Desks for Partner Departments.

"Partner Service Desks Agents" means the service desk agents employed by Partner Service Desks.

"Planned Actions" means those steps to be undertaken by the Contractor as established in the Corrective Action Plan.

"Progress Reports" means those periodic reports issued by the Contractor to indicate progress made against the Corrective Action Plan.

"Qualifying ESD Contacts" means legitimate contacts for Service Requests, Incident Reports and Change Requests made by Partner Service Desk Agents to the ESD via the following channels:

i. Telephone
ii. Email
iii. Email Listener

"Qualifying EUSD Contacts" means legitimate contacts for Service Requests, and Incident Reports made by End-User Service Desk Agents to the EUSD via the following channels:

i. Telephone
ii. Email

"Reduced Resource Charges Unit Rate" or "RRC Unit Rate" means with respect to a Base Service to be charged using a Monthly Variable Service Cost, the unit dollar credit rate for certain Service Volumes not experienced by SSC during a Measurement Period, as set forth in Section 2.2 of **ANNEX B – BASIS OF PAYMENT**.

"Reduced Resource Credits or "RRCs" means a reduced resource credit, as calculated in accordance with this Schedule B 1 – Pricing Provisions.

"Resolvable Contacts" are those incidents/service requests for which the ESD Service Desk Agents and the EUSD Service Desk Agents have the necessary training and access to tools required to resolve without assignment to Service Line Resolver Groups (in the Case of the ESD) or escalation to the ESD (in the case of the EUSD).

"Self-Service Portal Response Rate" means the proportion of Self-Service Portal contacts responded by Service Desk Agents within the Performance Target of entering the queue to the total number of Self-Service Portal contacts responded by Service Desk Agents.

"**Service Category"** means those distinct elements of the Service Desk Services for which the performance of the Contractor will be measured each month. Service Categories are established in Section 8 and Section 9 of **Schedule B 2 – Service Level Requirements**.

"Service Desk Agents" means those Contractor Personnel providing Single Point of Contact Services.

"Service Desk Services" means those services described in **Schedule A 1 – Service Desk Services**.

"Service Desk Services Operations Committee" will comprise senior executives from SSC and the Contractor (members to be determined) who will meet on a quarterly basis to discuss strategic and operational issues related to the Contract. The Executive Committee will be responsible for providing strategic direction to the Service Desk Services Contractor Operations Committee.

"Service Desk Services Operations Committee" will comprise business management and technology representatives from SSC and the Contractor. The Service Desk Services Operations Committee will be responsible for overseeing the operation of Service Desk Services, reviewing performance and addressing issues.

"Service Level Credit" means the amount owing by the Contractor to SSC as the result of a Service Level Failure.

"Service Level Failure" means the instance where the Level of Service for a given Service Level Category did not meet the Minimum Service Level in a month.

"Service Level Requirements" means the target level of performance for each Service Level Category. See Section 8 and Section 9 of **Schedule B 2 – Service Level Requirements**.

"Service Level Report" see Section 2 of **Schedule B 2 – Service Level Requirements**.

"Service Management Team" will comprise business management and technology staff from SSC and the Contractor. The Service Management Team will be responsible for overseeing the day-to-day operation of the in-scope Service Desk Services.

"Service Line Resolver Group" means those Government of Canada employees or contractors tasked with resolving issues impacting services provided by their service line. See Section 3.0 of **Schedule 13 – Types of Contacts Handled**.

"Single Point of Contact Services" means the toll-free infrastructure related support and electronic ticketing for reported Incidents, Service Requests and Requests for Change provided by the ESD, and the toll-free end-user support and electronic ticketing for reported Incidents and Service Requests provided by the EUSD.

"Telephone Call Abandonment Rate" means the proportion of telephone contacts abandoned after 60 seconds from entering the telephone queue to the total number of telephone contacts entering the telephone queue and remaining more than 60 seconds.

"Telephone Answer Rate" means the proportion of telephone contacts answered by Service Desk Agents within the Performance Target of entering the telephone queue to the total number of telephone contacts answered.

"Transition Milestone Delivery Date" means the established timeline for completion of Transition Service Milestones set forth in the Transition Project Plan.

"Transition Milestone Payment Amount" means the amount invoiced to SSC for successful delivery of a Transition Service Milestone.

"Transition Project Plan" means the agreed elements and timeline for completion of the Transition Service (see Appendix A of **Schedule A 3 – Transition Service**).

"Transition Service Milestone" means an agreed element of the Transition Project Plan bearing a Transition Milestone Delivery Date and a Milestone Payment Amount.

"Upset Limit" means the (+/-) range for which consistent Actual Service Volumes experienced outside the range will trigger a re-establishment of the Monthly Baseline Service Volume, Variable Service Unit Cost and Variable Service Cost Adjustments (ARC and Reduce RRC).

"Variable Service Cost Adjustment" means the cost adjustment to be applied when the Actual Service Volume for the Measurement Period is greater or less than the Dead Band (+/ 5% of Monthly Baseline Service Volume) for each month of the Measurement Period.

Schedule A 8 – System and Network Architecture

Shared Services Canada (SSC)

Schedule A 8 – System and Network Architecture

Table of Contents

List of Figures

Schedule A 8 – System and Network Architecture

This Schedule describes at a high level the technical architecture of how the Enterprise Service Desk (ESD) and End User Service Desk (EUSD) will be accessed in order to provide Service Desk Services described in **Schedule A 1 – Service Desk Services**. Employees, agents, sub-contractors and management of the Contractor and/or its Partner(s) (Contractor Personnel) working at the Contractor Premises will use their own computers to browse to a Web site which will be hosted on the Government of Canada Cloud network. Login access to the Website will require SSL connectivity. Contractor Personnel will connect to the Virtual Desktop Infrastructure (VDI) that will host the ITSM applications from their physical desktop. SSC may provide virtual desktops or virtualized applications or a combination as it sees fit. The following diagram represents a conceptual view of the distribution of the ESD and EUSD locations.

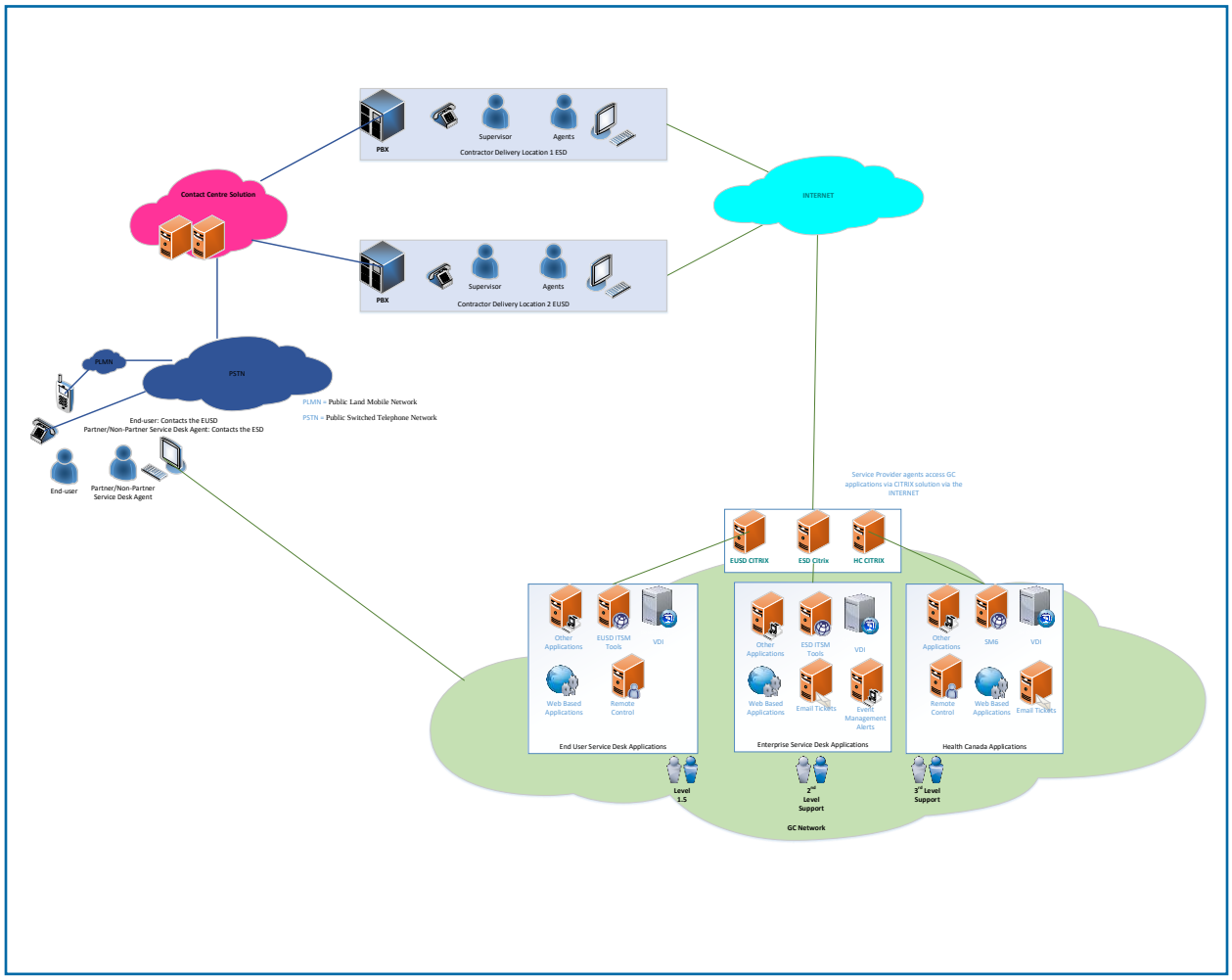


Figure 7: System and Network Architecture

1.0 Citrix Solution

1.1 Remote Access into GCNet

SSC will provide the Contractor with a remote access Virtual Desktop Infrastructure (VDI) solution. This solution will be accessible via the internet, providing Contractor Personnel located at the Contractor Premises with secure, managed access to the necessary tool(s), software and databases located within the Government of Canada Network (GCNet).

1.2 Remote Access to SSC Applications and Services

The VDI solution provided by SSC will offer sufficient performance and capacity to enable the Contractor to meet its service level obligations. Through the VDI, Contractor Personnel will be provided secure, managed access to GC systems and services including the HCCS, agent knowledge base and ITSM tools. SSC will provide credentials for access to all systems.

At their expense, the Contractor will set-up a third party second factor authenticator application. The SSC CITRIX solution, uses two-factor authentication based on RFC 6238 and supports the following list (Google authenticator (phone app), WinAuth (PC app), MS authenticator, Authy, LastPass) of two-step verification services using Time Based One-Time Password (TOTP).

For an agent to login into the SSC Environment via the Internet, they will enter their credentials (user and password) and then will be requested to enter their one time password. The user will generate their one time password using their supported application and then type that into the awaiting prompt to complete the authentication process.

2.0 Contact Centre Solution

The Hosted Contact Centre Service (HCCS) Telephony Platform provided by SSC, enables departments / agencies to interact with external and internal Government of Canada clients efficiently, effectively, and economically. Clients can contact Departments/Agencies using traditional telephony (PSTN, Centrex, PBX, or mobile) and alternate contact channels such as Voice over Internet Protocol (VoIP), email, text messaging, video, and social media. HCCS provides the infrastructure required by Departments/Agencies to create and to run their own contact centers. This infrastructure is virtual (cloud based) and requires minimal infrastructure on premises: End User Device (EUD) for agents, supervisors, and managers and connectivity.

At this time Session Initiation Protocol (SIP) trunking between the public internet and the Government of Canada is not authorized therefore a traditional telephony channel will be required at the Contractor interface point. The Contractor will control (e.g. queues) via a browser interface available from the CITRIX session.

SSC will provide a one-time training session to the Contractor on HCCS. It is the expectation that the Contractor will develop their own training material and train their personnel over the term of the contract on how to use HCCS.

3.0 Contractor Requirements

3.1 Infrastructure

At their expense, the Contractor is responsible for all configuration (tweaks, drivers, or other configuration), effort and cost to enable their infrastructure to support the SSC VDI solution. The Contractor must provide and make ready for use the technical infrastructure within the Contractor facilities as required to provide Service Desk Services where such technical infrastructure includes, but is not limited to, agent telephony

equipment, desktop infrastructure and the infrastructure required to interface the Contractor with the required government-provided data network services as set out in the target environment.

At their expense, the Contractor must provide and deliver physical desktop devices to their staff and SSC shall provide the secure desktop interface. This will take the form of a Virtual Desktop Infrastructure (VDI) provided, administered and operated by SSC. The Contractor must ensure that all desktop devices are installed with Citrix Workspace client software in order to allow Contractor Personnel to successfully establish connection to the SSC Environment.

3.2 Wide Area Network (WAN)

At their expense, the contractor shall be responsible for the provision of resilient internet connectivity to their facilities in a configuration that aligns to the service level requirements.

3.3 Disaster Recovery (DR) / Business Continuity Planning (BCP) Connectivity

At their expense, the Contractor shall provide connectivity required to support the DR/BCP.

3.4 Security

At their expense, the Contractor must comply with all of GC security policies and must complete the IT Security Risk Management process with a residual amount of risk acceptable to GC.

The Contractor will have the appropriate safeguards on their local infrastructure. SSC will require the Contractor to elaborate on (i) what safeguards will be in place, (ii) how those safeguards will be monitored over the Contract Term, and (iii) the reporting of monitoring results. The safeguards may include, but will not be limited to, the following:

- Strong passwords of at least 12 characters with symbols, numbers and characters;
- Firewall to protect their local network from incoming internet traffic;
- Up to date Antivirus software;
- Regular scans of the desktops for spyware;
- Software on the desktop is kept up to date;
- Ethical use of the desktops; and
- Unique user accounts.

3.5 Network Performance Reporting

The Contractor will be responsible for managing the performance and availability of their local and internet connection. The Contractor will continuously monitor and measure their network and internet connection to ensure that it is operating as needed to meet Service Level Requirements. The Contractor will perform dynamic trending of both historical and current data to show how the network is performing.

3.5.1 Network Performance Reporting Window

The Contractor will report on the Network Performance for each month of the Contract Term.

3.5.2 Network Performance Reporting Deadline

Within five (5) Federal Government Working Days (FGWD) after the end of each month, the Contractor will provide a Network Performance Report, in the prescribed manner.

3.5.3 Network Performance Report Content

At a minimum, the Network Performance Report must include the following:

a) Internet utilization at an hourly average and peak;

b) Latency experienced between the provider and SSC service;

c) Network packet loss and network jitter;

d) Experienced network speed;

e) Quality of service rules in place to prioritize the service desk traffic over other traffic. The report must indicate: (i) the quality of service rules in place, and (ii) when settings were changed during the month; and

f) Observations and any remedial actions the vendor will undertake to ensure the services to SSC are being met.

Schedule A 9 – Organization Structure

Shared Services Canada (SSC)

Schedule A 9 – Organization Structure

Table of Contents

List of Tables

Schedule A 9 – Organization Structure

1.0 Shared Services Canada (SSC) Overview and Organization Structure

1.1 SSC Overview

SSC's 2019-20 Departmental Plan (Link: SSC Departmental Plan) sets out the Department's priorities for the year, provides details on core responsibilities and significant activities, and how SSC plans to deliver results.

The Departmental Plan situates the environment in which SSC's Service Desk Services support the Department's mandate to deliver email, telecommunications, data centre and network services to all Partner Departments and limited services to Client Agencies/Organizations in a standardized manner to support the delivery of Government of Canada (GC) programs and services.

The Plan also presents information about SSC's resource management, operational structure, reporting framework.

1.2 SSC Organization Structure

SSC's Senior Leadership and high-level Organization Structure are provided in the following link: SSC Senior Leaders and Organization Structure. Service Desk Services are delivered through the Service Delivery and Management Branch in SSC.

2.0 Service Delivery and Management Branch (SDMB) Mandate and Organization Structure

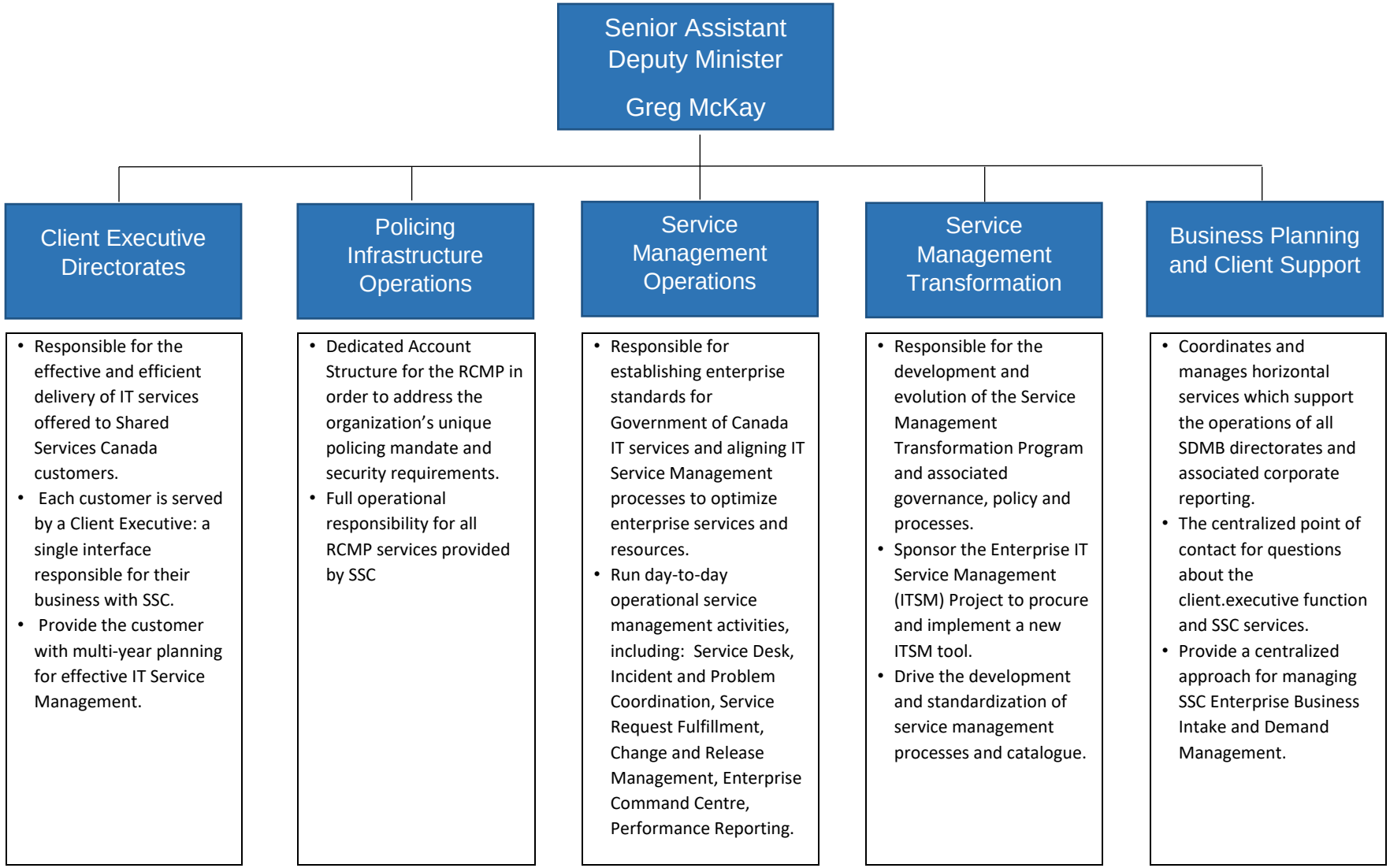
2.1 SDMB Vision

The Service Delivery and Management Branch will be the champions for driving SSC forward as a ***Customer-Centric***, ***Process-Driven***, ***Metrics-Based*** information technology service provider. We will apply the expertise of our staff, industry standard methodologies and process, coupled with world-class tools, to achieve these goals.

2.2 SDMB Mandate

The mandate of SDBM is to evolve Shared Services Canada's service management practices and process across the organization, with the goal of delivering excellence to our Government of Canada clients. We are the advocates of the client in holding SSC accountable for its service delivery.

2.3 Service Delivery and Management Branch Organizational Overview



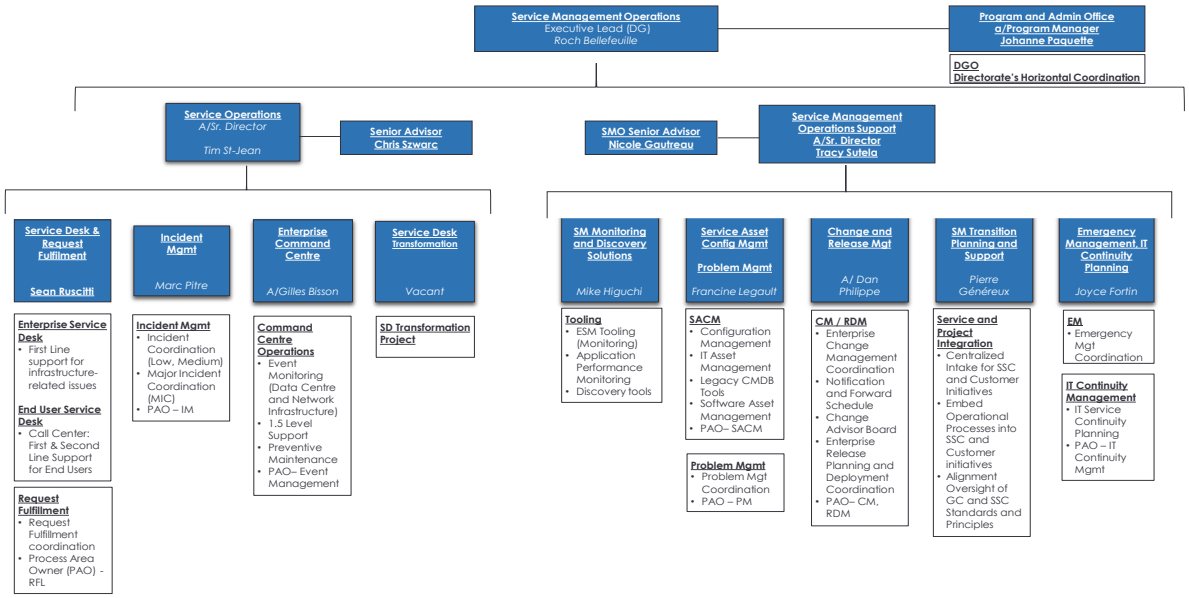
3.0 Service Management Operations (SMO) Mandate and Organization Structure

3.1 Service Management Operations Mandate

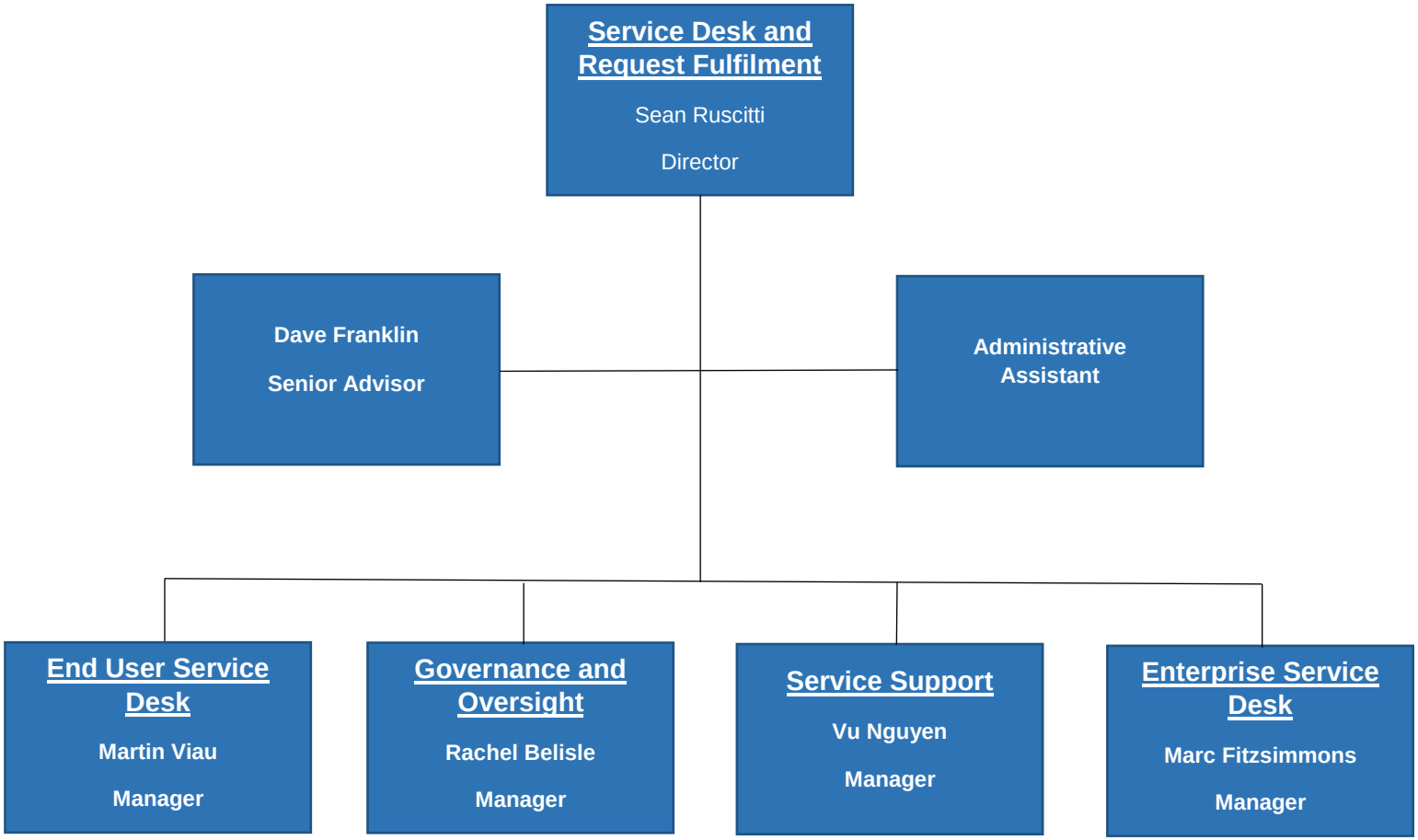
Table 55: Service Management Operations Mandate

Service Desk and Request Fulfilment	Incident Management	Enterprise Command Centre (ECC)	Monitoring and Discovery Solutions (MDS)
Single point of contact into SSC for all in-scope **service requests** and **incidents** providing timely response to fulfill, resolve or coordinate the resolution with SSC Service Lines and vendors. Manage Professional Services vendor who provides over 200 resources delivering Service Desk support.	**Incident Management Process Owner** coordinates investigation activities with Service Lines and Clients ensuring timely communications and resolutions. Major incident coordination support available 24/7/365.	**Event Management Process Owner** proactively monitors the operational status and availability of IT infrastructure 24/7/365. **Minimizes or avoids service interruptions** through the early detection of events and responds with the appropriate corrective actions. Manages Professional Services vendor who provides over 50 resources delivering ECC support.	Provides technical support for **monitoring and discovery tools.** Responsible for the strategy and plans to procure, consolidate and decommission monitoring and discovery tools.
Change and Release Management	**Service Asset and Configuration Management (SACM) & Problem Management**	**Emergency Management and IT Service Continuity**	**SM Transition Planning and Support (SMTPS)**
Change and Release Management Process Owner for all IT infrastructure changes. Provides governance and ensures process adherence from initial reporting, review, assessment, approval, release and final assessment.	**Asset and Configuration Management Process Owner** ensures all IT assets are properly controlled, asset information is accurate and relationships between assets is available. Responsible for the ITSM CMDB data model and the data integrity audit and verification. **Problem Management Process Owner** identifies and tracks corrective actions needed to determine and address root cause.	Advise, monitor and coordinate all activities related to **IT emergencies** that impact our client's ability to deliver services to Canadians. Coordinate the development and testing of **IT Continuity strategies and plans** while providing a standardized approach to IT Service Continuity across all clients.	PMD's entry point into SMO to ensure SSC's technical infrastructure is properly documented and aligned with the Service Line technical support teams to guarantee operational readiness for all new SSC services and projects.

3.2 SMO Organization Structure



3.3 Service Desk and Request Fulfilment (SDRF) Organization Structure



Schedule A 10 – Policies and Procedures

Shared Services Canada (SSC)

Schedule A 10 – Policies and Procedures

Table of Contents

List of Tables

Schedule A 10 – Policies and Procedures

1.0 Overview and Service Objectives

1.1 Overview

As a fully managed service provided on behalf of SSC to its employees and other federal workers in 43 federal departments and agencies, Service Desk Services must comply with all applicable Government of Canada legislation, policies and directives, as well as with SSC procedures.

This schedule includes, but is not limited to, a subset of key legislation and policy for which the managed service must be compliant.

1.2 Objective

SSC's objective is to ensure that:

- The Service Desk Services Managed Service fully complies with all applicable legislation, policy, standards, guidelines and procedures throughout the life of the contract;
- The Managed Service accommodates all changes to applicable legislation, policy, standards, guidelines and procedures throughout the life of the contract, including, but not limited to, those that may from time-to-time be identified by SSC; and
- In cases where an apparent conflict or discrepancy exists between any legislation, policy, directive or SSC procedure that they will be identified by the Contractor to permit SSC to make a determination and provide direction to the Contractor.

1.3 Policies and Procedures

Table 56: Policies and Procedures

	Subject	Title	Type	Reference	Current as Of (Date)
1	Accessibility	Accessibility Strategy for the Public Service of Canada	Policy	https://www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service/accessibility-public-service/accessibility-strategy-public-service-toc.html	2020-05-07
2	Accessibility	Accessible Canada Act	Legislation	https://laws.justice.gc.ca/eng/AnnualStatutes/2019_10/FullText.html	2019-06-21
3	Access to Information / Privacy	Access to Information Act	Legislation	https://laws-lois.justice.gc.ca/eng/acts/A-1/index.html	2020-05-17
4	Access to Information / Privacy	Access to Information Policy	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453	2014-09-22
5	Access to Information / Privacy	Interim Directive on the Administration of the Access to Information Act	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18310	2016-05-05
6	Access to Information / Privacy	Privacy Act	Legislation	https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html	2020-05-17
7	Access to Information / Privacy	Privacy Protection, Policy on	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510	2018-06-29
8	Access to Information / Privacy	Directive on Privacy Practices	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309	2010-04-01
9	Access to Information / Privacy	Directive on Privacy Impact Assessment	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308	2010-04-01
10	Access to Information / Privacy	Directive on Identity Management	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577	2019-07-01

	Subject	Title	Type	Reference	Current as Of (Date)
11	Network Use	Guideline on Acceptable Network and Device Use (GANDU)	Procedure	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27907&section=html	2016-05-30
12	Network Use	Operating Standard on the Acceptable Use of Cellular Devices	Procedure	http://service.ssc.gc.ca/en/policies_processes/policies/celluse	2018 (January)
13	Official Languages	Official Languages Act	Legislation	https://laws-lois.justice.gc.ca/eng/acts/o-3.01/FullText.html	2020-05-17
14	Open Government	Directive on Open Government	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28108	2014-10-09
15	Security	Policy on Government Security	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578	2019-07-01
16	Security	Standard on Security Screening	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115	2014-10-20
17	Service	Policy on Service and Digital	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603	2020-04-01
18	Service	Directive on Service and Digital	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601	2020-04-01
19	Values and Ethics	Values and Ethics Code for the Public Sector	Policy	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25049	2011-12-15

Schedule A 11 – Timing of Reporting and Events

Shared Services Canada (SSC)

Schedule A 11 – Timing of Reporting and Events

Table of Contents

List of Tables

Schedule A 11 – Timing of Reporting and Events

This Schedule lists reporting and events associated with the Service Desk Services described in **Schedule A 1 – Service Desk Services**.

1.0 Transition Reporting and Events

The following section lists the schedule of reporting and events associated with initial and transition activities described in:

- Schedule A 1 – Service Desk Services;
- Schedule A 3 – Transition Services; and
- Schedule A 15 – Privacy.

Table 57: List of Transition Reporting and Events

	Transition Reporting / Events	Category	Frequency	Deadline	Reference
1.0	Plan to Conform with Accessibility Requirements	Event	One-Time	Bid Close	RFP – Annex F
2.0	Preliminary Transition Project Plan + Project Status Process	Event	One-Time	Bid Close	Schedule A 3
3.0	Kick-Off Meeting	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
4.0	Transition Project Plan	Event	One-Time	Within ten (10) FGWDs of kick-off meeting	Schedule A 3
5.0	Transition Project Charter	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
6.0	Transition Project Staffing Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
7.0	Risk Mitigation Plan / Transition Risk Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
8.0	Weekly Program Office Transition Status Reports on Overall Adherence to Transition Plan	Reporting	Weekly	As agreed by SSC and the Contractor	Schedule A 3
9.0	Human Resources Sourcing and Retention Strategy	Event	One-Time	Within sixty (60) FGWDs of Contract Award	Schedule A 3
10.0	Program for Monitoring Customer Satisfaction	Event	One-Time	Within sixty (60) FGWDs of Contract Award	Schedule A 3
11.0	Quality Assurance Program	Event	One-Time	Within sixty (60) FGWDs of Contract Award	Schedule A 3
12.0	Stakeholder Engagement and Communications Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
13.0	Cutover Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
14.0	Readiness Assessment Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
15.0	Implementation Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
16.0	Integration and Testing Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
17.0	User Acceptance Test (UAT) Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
18.0	Transition-Out Project Plan	Event	One-Time	As agreed by SSC and the Contractor	Schedule A 3
19.0	Service Management Guide (Privacy / Security Breach Processes)	Event	One Time	As agreed by SSC and the Contractor	Schedule A 15
20.0	Agreement on Performance Measures (Service Level Requirements, Key Performance Indicators and Relationship Health Check Indicators)	Event	One Time	Within sixty (60) FGWDs of Contract Award	Schedule A 3
21.0	Privacy Management Plan	Event	One Time	Within sixty (60) FGWDs of Contract Award	Schedule A 15
22.0	Privacy Impact Assessment	Event	One Time	Within sixty (60) FGWDs of Contract Award	Schedule A 15
23.0	Disaster Recovery Plan	Event	One Time	Within one hundred and twenty (120) FGWDs of Contract Award	Schedule A 1

2.0 Periodic Reporting and Events

The following section lists the schedule of reporting and events associated with periodic activities described in:

- Schedule A 1 – Service Desk Services;
- Schedule A 2 – Service Management Services;
- Schedule A 4 – Governance and Relationship Management Services;
- Schedule A 8 – System and Network Architecture;
- Schedule A 15 – Privacy;
- Schedule B 2 – Service Level Requirements; and
- Schedule B 4 – Reporting.

Table 58: List of Periodic Reporting and Events

	Periodic Reporting / Events	Category	Frequency	Deadline	Reference
1.0	Update Metrics Repository with analytic data	Event	As Required	Concurrent with preparation of KPI / SLA reports	Schedule B 4
2.0	Service Level Reporting (SLR)	Reporting	Monthly	Five (5) FGWDs after end of each month	Schedule B 2/4
3.0	Previous Day Key Performance Indicators (KPIs) Reporting	Reporting	Daily	Within one (1) FGWD	Schedule B 4
4.0	Previous Week Key Performance Indicators (KPIs) Reporting	Reporting	Daily	Within one (1) FGWD from end of reporting period	Schedule B 4
5.0	Previous Month Key Performance Indicators (KPIs) Reporting	Reporting	Daily	Within five (5) FGWDs from end of reporting period	Schedule B 4
6.0	Update secure common repository for storage and retention of all SLR and KPI Reports	Event	As Required	Concurrent with completion of KPI / SLA reports	Schedule B 4
7.0	Network Performance Report	Reporting	Monthly	Five (5) FGWDs after end of each month	Schedule A 8
8.0	Semi-Annual Review of Service Level Credits	Event	Semi-annual	As agreed by SSC and the Contractor	Schedule B 2
9.0	Semi-Annual Review of Key Performance Indicators	Event	Semi-annual	As agreed by SSC and the Contractor	Schedule A 4
10.0	Privacy Breach Report	Reporting	Dictated by SSC	As agreed by SSC and the Contractor	Schedule A 15
11.0	Annual Disaster Recovery Testing	Event	Annually	At Contractor's discretion with appropriate notification to SSC	Schedule A 1
12.0	Annual Confirmation of Disaster Recovery Testing Report	Reporting	Annually	Within two (2) FGWDs of the Annual Disaster Recovery Test [see 9.0 – Table 3]	Schedule A 1
13.0	Executive Committee Meeting	Event	Quarterly	As agreed by SSC and the Contractor	Schedule A 4
14.0	Provide and Implement Innovative / New idea	Event	Quarterly	As agreed by SSC and the Contractor	Schedule A 1
15.0	Operations Committee Meeting	Event	Monthly	As agreed by SSC and the Contractor [Note: may meet more frequently at SSC's discretion]	Schedule A 4
16.0	Service Management Team	Event	Weekly	As agreed by SSC and the Contractor [Note: may meet on a different basis where agreed by SSC and the Contractor]	Schedule A 4

3.0 Ad Hoc Reporting and Events

The following section lists the schedule of reporting and events associated with ad hoc activities described in:

- Schedule A 1 – Service Desk Services;
- Schedule A 2 – Service Management Services;
- Schedule A 4 – Governance and Relationship Management Services;
- Schedule A 15 – Privacy; and
- Schedule B 2 – Service Level Requirements.

Table 59: List of Ad Hoc Reporting and Events

	Ad Hoc Reporting / Events	Category	Frequency	Deadline	Reference
1.0	Immediate notification of realized or imminent failure to meet Minimum Service Level in any Service Level Category	Reporting	As Required	Immediate	Schedule B 2
2.0	Root Cause Analysis Report	Reporting	As Required	Within five (5) FGWDs from date of notification [see 1.0 – Table 3]	Schedule B 2
3.0	Corrective Action Plan	Event	As Required	Within ten (10) FGWDs from date of notification [see 1.0 – Table 3]	Schedule B 2
4.0	Implementation of Corrective Action Plan	Event	As Required	Within twenty (20) FGWDs from publication of Corrective Action Plan [see 3.0 – Table 3.0]	Schedule B 2
5.0	Progress Reports against the Corrective Action Plan	Event	Weekly	Schedule agreed by SSC and the Contractor	Schedule B 2
6.0	Notification of potential impact on Service Levels by condition of Force Majeure	Reporting	As required	Immediate	Schedule B 2
7.0	Update to Privacy Management Plan	Event	As Required	Within twenty (20) FGWDs of Request by SSC	Schedule A 15
8.0	Security Incident and Privacy Breaches (including activities undertaken to counter-act)	Event	As required	Immediate	RFP Security Clauses
9.0	Security Patching	Event	As required	Within 14 FGWDs from release and within 48 hours for all urgent/critical patches as identified by SSC.	Schedule A 1
10.0	Remediation Plan for Failure of Annual Disaster Recovery Testing	Event	As required	Within ten (10) FGWDs from date of the test	Schedule A 1
11.0	Participation and support during emergency/crises situations including reporting and status of the service desk	Event	As required	Immediately	Schedule A 1
12.0	Re-establishment of: (i) Monthly Baseline Service Volume (ii) Variable Service Unit Cost, and (iii) Variable Service Cost Adjustments (ARC and RRC)	Event	As required	Within 90 Calendar days from the last day of the third consecutive month triggering the Re-establishment	Schedule B 1

Schedule A 12 – Customers Supported

Shared Services Canada (SSC)

Schedule A 12 – Customers Supported

Table of Contents

List of Tables

Schedule A 12 – Customers Supported

This Schedule describes the Enterprise Service Desk Customers (ESD Customers) supported by the Enterprise Service Desk (Section 1.0 ESD Customers) and the End User Service Desk Customers (EUSD Customers) supported by the End User Service Desk (Section 2.0 EUSD Customers).

1.0 ESD Customers

Shared Services Canada (SSC) is responsible for delivering mandated email, telecommunications, data centre and network services to Partner Departments and limited services to Agencies/Organizations in a consolidated and standardized manner to support the delivery of Government of Canada programs and services.

This section describes the ESD Customers (Partner Departments and Client Agencies/Organizations) currently supported by the ESD for mandated services.

1.1 ESD Supported Partners: Fully On-boarded (Using E-mail Listener)

The ESD currently supports Partner Departments that have had their legacy ITSM tool on-boarded to the ESD ITSM Tool. Partner Service Desk Agents utilize the following contact channels:

- Self-service Portal to ESD ITSM Tool;
- Phone to ESD (1-855-830-7782 option 1) / Mobile Travel Devices (MTD) (1-416-861-8594);
- ESD E-mail (SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca) to ESD ITSM Tool; and
- E-mail Listener operating as a bridge between Partner ITSM Tool and ESD ITSM Tool.

Table 60: Fully On-boarded Partner Departments (Using E-mail Listener)

	Department Name	Department Abbr.
1	Agriculture and Agri-Food Canada	AAFC
2	Canadian Food Inspection Agency	CFIA
3	Canadian Heritage	PCH
4	Canadian Northern Economic Development Agency	CanNor
5	Canadian Space Agency	CSA
6	Correctional Service Canada	CSC
7	Employment and Social Development Canada	ESDC
8	Environment and Climate Change Canada (formerly EC)	ECCC
9	Federal Economic Development Agency for Southern Ontario (FedDev Ontario)	FedDevOn
10	Fisheries and Oceans Canada	DFO
11	Health Canada	HC
12	Immigration, Refugees and Citizenship Canada (formerly CIC)	IRCC
13	Crown Indigenous Relations and Northern Affairs Canada (formerly INAC)	CIRNAC
14	Innovation, Science and Economic Development Canada (formerly IC)	ISED
15	National Research Council Canada	NRC
16	Natural Resources Canada	NRCan
17	Parks Canada	PC
18	Public Health Agency of Canada	PHAC

	Department Name	Department Abbr.
19	Veterans Affairs Canada	VAC
20	Statistics Canada	STATCAN

1.2 ESD Supported Partners: Fully On-boarded (Not using E-mail Listener)

The ESD currently supports Partner Departments that have fully on-boarded their legacy ITSM tool to the ESD ITSM Tool. Partner Service Desk Agents utilize the following contact channels:

- Self-service Portal to ESD ITSM Tool;
- Phone to ESD (1-855-830-7782 option 1) / Mobile Travel Devices (1-416-861-8594); and
- ESD E-mail (SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca)

  to ESD ITSM Tool for Enterprise Services.

Table 61: Fully On-boarded Partner Departments (Not Using E-mail Listener)

	Department Name	Department Abbr.
21	Atlantic Canada Opportunities Agency	ACOA
22	Canada Economic Development for Quebec Regions	CEDQ
23	Canadian Nuclear Safety Commission	CNSC
24	Department of Finance Canada	FIN
25	Financial Transactions and Reports Analysis Centre of Canada	FINTRAC
26	Immigration and Refugee Board of Canada	IRB
27	Passport Canada	PPTC
28	Public Safety Canada	PS
29	Transport Canada	TC
30	Western Economic Diversification Canada	WD

1.3 ESD Supported Partners: Partially On-boarded (Formerly Government Operations Portfolio)

The ESD currently supports former Partner Departments of the Government Operations Portfolio (GOP) that have partially on-boarded their legacy ITSM tool to the ESD ITSM Tool. Partner Service Desk Agents utilize the following contact channels:

- Self-service Portal to ESD ITSM Tool for on-boarded services;
- Phone to ESD (1-855-830-7782 option 2) / Mobile Travel Devices (416-861-8594); and
- National Service Desk E-mail (SSC.nationalservicedesk-bureaudeservicenational.SPC@canada.ca) to InfoWeb Tool.

Former Partner Departments of the GOP are supported through the National Service Desk (NSD) which is a virtual desk within the ESD using the InfoWeb Tool.

Table 62: Partially On-boarded Partner Departments

	Department Name	Department Abbr.
31	Canada School of Public Service	CSPS
32	Department of Justice	DOJ
33	Infrastructure Canada	INFC
34	Library and Archives Canada	LAC
35	Privy Council Office	PCO
36	Public Service Commission of Canada	PSC
37	Public Services and Procurement Canada (formerly PWGSC)	PSPC
38	Shared Services Canada	SSC
39	Treasury Board of Canada Secretariat	TBS

1.4 ESD Supported Partners: On-boarded Some Enterprise Services

The ESD currently supports Partner Departments that (i) have on-boarded their legacy ITSM tool to the ESD ITSM Tool for some Enterprise Services, (ii) retain SSC resources using the Legacy ITSM Tool for non-Enterprise Services. Partner Service Desk Agents utilize the following contact channels:

- Self-service Portal to ESD ITSM Tool for Enterprise Services;
- Phone to ESD or Enterprise Services (1-855-830-7782 option 1) / Mobile Travel Devices (416-861-8594); and
- ESD E-mail (SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca) to ESD ITSM Tool for Enterprise Services.

Table 63: Partner Departments with some Enterprise Services On-boarded

	Department Name	Department Abbr.
40	Canada Border Services Agency	CBSA
41	Canada Revenue Agency	CRA
42	Global Affairs Canada (formerly DFAIT)	GAC
43	National Defence and the Canadian Armed Forces	DND
44	Royal Canadian Mounted Police	RCMP

1.5 ESD Supported Non-partner Clients: Limited Enterprise Services

The ESD currently supports non-partner client agencies/organizations that subscribe for Network and Toll-free Services. Non-partner Service Desk Agents utilize the following contact channels:

Toll-Free/Network etc.

- Phone to ESD (1-855-830-7782 option 1) / Mobile Travel Devices (416-861-8594);
- ESD E-mail (SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca) to ESD ITSM Tool for Enterprise Services;
- Shared Metropolitan Service (SMS) and MyKey/PKI;
- Phone to ESD (1-855-830-7782 option 2) / Mobile Travel Devices (416-861-8594); and
- National Service Desk E-mail (SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca) to InfoWeb Tool.

Table 64: Non-partner Agencies / Organizations Subscribing to Limited Service Offerings

	Agency/Organization Name	Agency/ Org. Abbr.
1	Assisted Human Reproduction Canada	AHRC
2	Atlantic Pilotage Authority	APA
3	Atomic Energy of Canada Limited	AECL
4	Bank of Canada	BoC
5	Business Development Bank of Canada	BDC
6	Canada Coast Guard	CCG
7	Canada Deposit Insurance Corporation	CDIC
8	Canada Industrial Relations Board	CIRB
9	Canada Lands Company Limited	CLC
10	Canada Mortgage and Housing Corporation	CMHC
11	Canada Post	CPC
12	Canadian Air Transport Security Authority	CATSA
13	Canadian Artists and Producers Professional Relations Tribunal	CAPPRT
14	Canadian Centre for Cyber Security	CCCS
15	Canadian Centre for Occupational Health and Safety	CCOHS
16	Canadian Commercial Corporation	CCC
17	Canadian Dairy Commission	CDC
18	Canadian Environmental Assessment Agency	CEAA
19	Canadian Forces Grievance Board	CFGB
20	Canadian Grain Commission	CGC
21	Canadian Human Rights Commission	CHRC
22	Canadian Human Rights Tribunal	CHRT
23	Canadian Institutes of Health Research	CIHR
24	Canadian Intergovernmental Conference Secretariat	CICS
25	Canadian International Development Agency	CIDA
26	Canadian International Trade Tribunal	CITT
27	Canadian Judicial Council	CJC
28	Canadian Museum of History	CMH
29	Canadian Museum of Nature	CMN
30	Canadian Radio-television and Telecommunications Commission	CRTC
31	Canadian Tourism Commission	CTC
32	Canadian Transportation Agency	CTA
33	Civilian Review and Complaints Commission	CRCC
34	Communications Research Centre Canada	CRC
35	Competition Bureau Canada	CB
36	Copyright Board of Canada	CB
37	Courts Administration Service	CAS
38	Defense Construction Canada	DCC
39	Defense Research and Development Canada	DRDC
40	Elections Canada	Elections
41	Environmental Protection Review Canada	EPRC
42	Export Development Canada	EDC
43	Farm Credit Canada	FCC
44	Federal Court of Canada	FC

	Agency/Organization Name	Agency/ Org. Abbr.
45	Financial Consumer Agency of Canada	FCAC
46	Halifax Port Authority	HPA
47	House of Commons	HOC
48	Indian Residential Schools Adjudication Secretariat	IRSAD
49	International Development Research Centre	IDRC
50	International Joint Commission	IJC
51	Library of Parliament	LoP
52	Marine Atlantic	MarineAtlantic
53	Military Grievances External Review Committee	MGERC
54	Military Police Complaints Commission	MPCC
55	National Battlefields Commission	NBC
56	National Capital Commission	NCC
57	National Council of Welfare	NCW
58	National Energy Board	NEB
59	National Film Board of Canada	NFB
60	National Joint Council	NJC
61	National Search and Rescue Secretariat	NSS
62	Natural Sciences and Engineering Research Council of Canada	NSERC
63	Occupational Health and Safety Tribunal Canada	OHSTC
64	Office of the Auditor General of Canada	OAG
65	Office of the Chief Electoral Officer	ELECTC
66	Office of the Commissioner for Federal Judicial Affairs	FJA
67	Office of the Commissioner of Lobbying of Canada	OCL
68	Office of the Commissioner of Official Languages	OCOL
69	Office of the Commissioner Review Tribunals Canada Pension Plan/Old Age Security	OCRT
70	Office of the Conflict of Interest and Ethics Commissioner	CIE
71	Office of the Correctional Investigator	OCI
72	Office of the Governor general's secretary	GG
73	Office of the Information Commissioner of Canada	OIC
74	Office of the Privacy Commissioner of Canada	OPC
75	Office of the Public Sector Integrity Commissioner of Canada	PSIC
76	Office of the Secretary to the Governor General	OSGG
77	Office of the Superintendent of Financial Institutions Canada	OSFI
78	Office of the Umpire	OU
79	Ontario Federal Council	OFC
80	Parole Board of Canada	NPB
81	Passport Office	
82	Patented Medicine Prices Review Board	PMPRB
83	Pension Appeals Board	PAB
84	Polar Knowledge Canada	POLAR
85	Policy Horizons Canada	Horizons
86	Public Safety Canada	
87	Public Sector Pension Investment Board	PSP Investments
88	Public Servants Disclosure Protection Tribunal Canada	PSDPTC
89	Public Service Labour Relations Board	PSLRB

	Agency/Organization Name	Agency/ Org. Abbr.
90	Public Service Staffing Tribunal	PSST
91	Public-Private Partnership Canada	PPP Canada
92	Registry of the Competition Tribunal	CT
93	Registry of the Public Servants Disclosure Protection Tribunal	PSDPT
94	Registry of the Specific Claims Tribunal of Canada	SCT
95	Royal Canadian Mint	MINT
96	Security Intelligence Review Committee	SIRC
97	Seniors Canada	
98	Social Sciences and Humanities Research Council of Canada	SSHRC
99	Social Security Tribunal	SST
100	Department for Women and Gender Equality (WAGE)	WAGE
101	Supreme Court of Canada	SCC
102	Taxpayers' Ombudsman (Office of the)	OTO
103	Telefilm Canada	TFC
104	Transportation Appeal Tribunal of Canada	TATC
105	Transportation Safety Board of Canada	TSB
106	Truth and Reconciliation Commission	TRC

The number of ESD Customers supported by the ESD will fluctuate over the term of the engagement. Material changes in the number of supported end-users and associated contact volumes will be accommodated through the volume banded price structure.

2.0 EUSD Customers

The EUSD provides end-user support to five departments. EUSD Customers currently supported by the EUSD are as follows:

Table 65: EUSD End-User Population

	Customer Name [Department/Agency]	Department Abbr.	End-User Population [Federal Public Service][Note 1]
1.	Public Service and Procurement Canada	PSPC	15,721
2.	Health Canada (Public Health Agency of Canada and Patented Medicine Prices Review Board)	HC (including PHAC and PMPRB)	13,247
3.	Shared Services Canada	SSC	6,528
4.	Canada School of Public Service	CSPS	620
5.	Infrastructure Canada	INFC	514
	TOTAL		**36,630**

***Note 1**: Population of Federal Public Service by Department as at March 31, 2019 (Source: Treasury Board of Canada Secretariat) [https://www.canada.ca/en/treasury-board-secretariat/services/innovation/human-resources-statistics/population-federal-public-service-department.html]*

The end-user population supported by the EUSD will fluctuate over the term of the engagement. Material changes in the number of supported end-users and associated contact volumes will be accommodated through the volume banded price structure.

End-users contact the EUSD through the following channels:

Table 66: EUSD Contact Channels

		Department Abbr.	Phone Numbers	Email Address	Self-service Catalogue
1.	Public Service and Procurement Canada	PSPC	**Toll Free:** 1-866-995-6030 **Direct Local:** N/A **External Transfer:** 1-855-830-7782 (after hours)	N/A	Office System Service Request Online (OSSRO)
	Public Service and Procurement Canada – Minister's Regional Office (MRO) [Standard PSPC Support with higher priority on call receipt]	PSPC	**Toll Free:** 1-855-242-3554 **Direct Local:** N/A **External Transfer:** 1-855-830-7782 (after hours)	N/A	Office System Service Request Online (OSSRO)
	Office of the Procurement Ombudsman (OPOC) [Standard PSPC Support with higher priority on call receipt]	PSPC	**Toll Free:** 1-833-228-9071 **Direct Local:** 613-947-6272 **External Transfer:** 1-855-830-7782 (after hours)	N/A	Office System Service Request Online (OSSRO)
2.	Health Canada	HC	**Toll Free:** 1-800-416-0358 **Direct Local:** 613-954-8718 **External Transfer:** N/A (after hours)	hc.nationalservicedesk-bureaudeservicenational.sc@canada.ca	N/A
3.	Shared Services Canada	SSC	**Toll Free:** 1-855-591-0550 **Direct Local:** N/A **External Transfer:** 1-855-830-7782 (after hours)	N/A	Government of Canada Service Express (GCSX)
4.	Canada School of Public Service	CSPS	**Toll Free:** 1-833-228-9068 **Direct Local:** 613-943-6236 **External Transfer:** 1-855-830-7782 (after hours)	**Request Management:** csps.itservicedeskbureaudeserviceti.efpc@canada.ca	N/A
5.	Infrastructure Canada	INFC	**Toll Free:** 1-833-228-9069 **Direct Local:** 613-941-2427 **External Transfer:** 1-855-830-7782 (after hours)	**Request Management:** infc.itservices-servicesti.infc@canada.ca	N/A

		Department Abbr.	Phone Numbers	Email Address	Self-service Catalogue
6.	Sigma		**Toll Free:** 1-866-712-1502 **Direct Local:** N/A **External Transfer:** N/A (after hours)		

Schedule A 13 – Types of Contacts Handled

Shared Services Canada

Schedule A 13 – Types of Contacts Handled

Table of Contents

List of Tables

Schedule A 13 – Types of Contacts Handled

This Schedule describes the types of contact handled by the Enterprise Service Desk (ESD) and End User Service Desk (EUSD) in the provision of Service Desk Services described in **Schedule A 1 – Service Desk Services**.

1.0 ESD Contacts Handled

The following Tables list the types of incidents/service requests handled by the Enterprise Service Desk (ESD). In addition, the table indicates those interactions that are expected to be resolved by the ESD ("Resolvable Contacts") and those that are expected to be assigned to Service Line Resolver Groups ("Non-Resolvable Contacts").

Resolvable Contacts are those incidents/service requests for which the ESD Service Desk Agents have the necessary training and access to tools required to resolve without assignment to Service Line Resolver Groups.

For greater clarity, Non-resolvable Contacts do not include contacts that inadvertently arrive at the ESD but should instead have gone to another desk or organization ("Out-of-Scope Contacts"). Out-of-Scope contacts should be re-directed to the appropriate desk or organization through manual or automatic means (i.e. ACD).

These lists are subject to change at the discretion of SSC. Changes will be reviewed and agreed with the Contractor before those changes are applied.

In the instance of incidents/service requests not listed in the tables below, the Contractor is required to provide support and resolution within the performance targets keeping the customer experience intact. The Contractor is then responsible for addressing these "new" incidents/service requests with SSC in order to update the contact list as per the agreement between SSC and the Contractor.

1.1 ESD - Incident Management (Resolvable vs. Non-resolvable)

The following Table lists the types of incidents handled by ESD Service Desk Agents:

Table 67 ESD: Contacts Handled – Incident Management

	Type of Contact	Detail	Action	Disposition
1	TELECOM	Mobile	Triage, assess, synthesize, assign	Non-Resolvable
2	TELECOM	Fixed Line	Triage, assess, synthesize, assign	Non-Resolvable
3	TELECOM	Satellite Device	Triage, assess, synthesize, assign	Non-Resolvable
4	NETWORK	WAN	Triage, assess, synthesize, assign	Non-Resolvable
5	NETWORK	LAN	Triage, assess, synthesize, assign	Non-Resolvable
6	NETWORK	Wi-Fi	Triage, assess, synthesize, assign	Non-Resolvable
7	NETWORK	Cloud Solutions	Triage, assess, synthesize, assign	Non-Resolvable
8	MAINFRAME	Mainframe	Triage, assess, synthesize, assign	Non-Resolvable
9	SECURITY	PKI	Triage, assess, synthesize, assign	Non-Resolvable
10	SECURITY	Firewall	Triage, assess, synthesize, assign	Non-Resolvable
11	SECURITY	VPN	Triage, assess, synthesize, assign	Non-Resolvable
12	SECURITY	Remote Access	Triage, assess, synthesize, assign	Non-Resolvable
13	SECURITY	Cyber	Triage, assess, synthesize, assign	Non-Resolvable
14	MIDRANGE	Midrange	Triage, assess, synthesize, assign	Non-Resolvable
15	FILE AND PRINT	File and Print	Triage, assess, synthesize, assign	Non-Resolvable
16	SUPERCOMPUTING	HPC	Triage, assess, synthesize, assign	Non-Resolvable
17	APPLICATIONS	Applications	Triage, assess, synthesize, assign	Non-Resolvable
18	MESSAGING	Email Legacy	Triage, assess, synthesize, assign	Non-Resolvable
19	MESSAGING	ETI	Triage, assess, synthesize, assign	Non-Resolvable

	Type of Contact	Detail	Action	Disposition
20	VIDEO CONFERENCING / TELEPRESENCE	Video Conferencing / Telepresence	Triage, assess, synthesize, assign	Non-Resolvable
21	STORAGE	Storage	Triage, assess, synthesize, assign	Non-Resolvable
22	HARDWARE	Hardware	Triage, assess, synthesize, assign	Non-Resolvable
23	FACILITIES	HVAC	Triage, assess, synthesize, assign	Non-Resolvable
24	FACILITIES	Data Centre	Triage, assess, synthesize, assign	Non-Resolvable

1.2 ESD - Request Fulfilment (Resolvable vs. Non-resolvable)

The following Table lists the types of service requests handled by ESD Service Desk Agents:

Table 68: ESD Contacts Handled – Request Fulfilment

	Type of Contact	Detail	Action	Disposition
1	TELECOM	Mobile	Triage, assess, synthesize, assign	Non-Resolvable
2	TELECOM	Fixed Line	Triage, assess, synthesize, assign	Non-Resolvable
3	TELECOM	Satellite Device	Triage, assess, synthesize, assign	Non-Resolvable
4	NETWORK	WAN	Triage, assess, synthesize, assign	Non-Resolvable
5	NETWORK	LAN	Triage, assess, synthesize, assign	Non-Resolvable
6	NETWORK	Wi-Fi	Triage, assess, synthesize, assign	Non-Resolvable
7	NETWORK	Cloud Solutions	Triage, assess, synthesize, assign	Non-Resolvable
8	MAINFRAME	Mainframe	Triage, assess, synthesize, assign	Non-Resolvable
9	SECURITY	PKI	Triage, assess, synthesize, assign	Non-Resolvable
10	SECURITY	Firewall	Triage, assess, synthesize, assign	Non-Resolvable
11	SECURITY	VPN	Triage, assess, synthesize, assign	Non-Resolvable
12	SECURITY	Remote Access	Triage, assess, synthesize, assign	Non-Resolvable
13	SECURITY	MyKey	Triage, assess, synthesize, assign	Non-Resolvable
14	SECURITY	Cyber	Triage, assess, synthesize, assign	Non-Resolvable
15	MIDRANGE	Midrange	Triage, assess, synthesize, assign	Non-Resolvable
16	FILE AND PRINT	File and Print	Triage, assess, synthesize, assign	Non-Resolvable
17	SUPERCOMPUTING	HPC	Triage, assess, synthesize, assign	Non-Resolvable
18	APPLICATIONS	Applications	Triage, assess, synthesize, assign	Non-Resolvable
19	MESSAGING	Email Legacy	Triage, assess, synthesize, assign	Non-Resolvable
20	MESSAGING	ETI	Triage, assess, synthesize, assign	Non-Resolvable
21	VIDEO CONFERENCING / TELEPRESENCE	Video Conferencing / Telepresence	Triage, assess, synthesize, assign	Non-Resolvable
22	STORAGE	Storage	Triage, assess, synthesize, assign	Non-Resolvable
23	FACILITIES	HVAC	Triage, assess, synthesize, assign	Non-Resolvable
24	FACILITIES	Data Centre	Triage, assess, synthesize, assign	Non-Resolvable
25	PASSWORD RESET	Mainframe PSPC SPS	Perform	Resolvable
26	PASSWORD RESET	PSPC Siebel	Perform	Resolvable
27	PASSWORK RESET	OTHER	Triage, assess, synthesize, assign	Non-Resolvable
28	PASSWORD RESET	Mainframe Regional Payment System (RPS)	Perform	Resolvable
29	PASSWORD RESET	Phoenix / CWA	Triage, assess, synthesize, assign	Non-Resolvable
30	PASSWORD RESET	FTP account	Triage, assess, synthesize, assign	Non-Resolvable

	Type of Contact	Detail	Action	Disposition
31	PASSWORD RESET	ECD	Perform	Resolvable
32	PASSWORD RESET	PSPC Crown Corporation Secure Portal (DCT)	Perform	Resolvable
33	PASSWORD RESET	CCPULSE	Perform	Resolvable
34	PASSWORD RESET	GCPENS (Penfax, Penmod, Workforce Mgmt)	Perform	Resolvable
35	PASSWORD RESET	Get-Answers	Perform	Resolvable
36	PASSWORD RESET	E-Snap	Perform	Resolvable
37	PASSWORD RESET	InfoMan	Perform	Resolvable
38	PASSWORD RESET	Pay Mainframe (Online Pay, SPAY)	Perform	Resolvable
39	PASSWORD RESET	Common Departmental Financial System (CDFS)	Perform	Resolvable
40	PASSWORD RESET	GBS (Government Banking System Web)	Perform	Resolvable
41	PASSWORD RESET	Automated Buyer Environment (ABE)	Perform	Resolvable
42	PASSWORD RESET	Acquisition Information Services (AIS)	Perform	Resolvable
43	PASSWORD RESET	PSSA Annuitant Pensions (ANNPEN) (CV66)	Perform	Resolvable
44	PASSWORD RESET	Banking Facility System (BFS)	Perform	Resolvable
45	PASSWORD RESET	Central Agencies Information System / DB2 Relational (CAIS/R)	Perform	Resolvable
46	PASSWORD RESET	Communication Canada Interface (CCI)	Perform	Resolvable
47	PASSWORD RESET	Central Index (CENINDX)	Perform	Resolvable
48	PASSWORD RESET	Central Financial Management Reporting System (CFMRS)	Perform	Resolvable
49	PASSWORD RESET	Canadian Forces Pay Allotment (DND PAY) (CFPA)	Perform	Resolvable
50	PASSWORD RESET	Citizenship Registration Index (CICCRI)	Perform	Resolvable
51	PASSWORD RESET	Canadian Intellectual Properties Office Batch (CIPOBTCH)	Perform	Resolvable
52	PASSWORD RESET	Customer Information Service (CIS)	Perform	Resolvable
53	PASSWORD RESET	Contract Retrieval (CNTRS)	Perform	Resolvable
54	PASSWORD RESET	Contributor (CONT)	Perform	Resolvable
55	PASSWORD RESET	Canada Pension Plan (CPP)	Perform	Resolvable
56	PASSWORD RESET	Common Reference Information System (CRIS)	Perform	Resolvable
57	PASSWORD RESET	Canada Savings Bonds (CSB)	Perform	Resolvable
58	PASSWORD RESET	Central System Mailbox (CSM)	Perform	Resolvable
59	PASSWORD RESET	Direct Deposit (DDIS)	Perform	Resolvable
60	PASSWORD RESET	CFSA Annuitant Pension (DND) (DNDPEN)	Perform	Resolvable
61	PASSWORD RESET	Electronic Authorization & Authentication (EAA)	Perform	Resolvable

	Type of Contact	Detail	Action	Disposition
62	PASSWORD RESET	Employee Immigration Canada (EIC)	Perform	Resolvable
63	PASSWORD RESET	Elections Payments	Perform	Resolvable
64	PASSWORD RESET	Estimates & Elections (ESTEL)	Perform	Resolvable
65	PASSWORD RESET	FINCON	Perform	Resolvable
66	PASSWORD RESET	Financial Management System (RPS) (FMS28)	Perform	Resolvable
67	PASSWORD RESET	Financial Management System / Relational (RPS/R) (FMS/R)	Perform	Resolvable
68	PASSWORD RESET	Government Electronic Data Interchanging Server (GEDIS)	Perform	Resolvable
69	PASSWORD RESET	Generic Utilities Services for FIS (GUS)	Perform	Resolvable
70	PASSWORD RESET	Inmates Pay Accounting (INPAC)	Perform	Resolvable
71	PASSWORD RESET	Inmate Accounting System (IAS)	Perform	Resolvable
72	PASSWORD RESET	Income Security Programs Redesign (ISPR)	Perform	Resolvable
73	PASSWORD RESET	Judges Pension (Annuitant) (JUDPEN)	Perform	Resolvable
74	PASSWORD RESET	PAC / Leave Reporting System (LRSL)	Perform	Resolvable
75	PASSWORD RESET	PAC / Leave Without Pay System (LWOP)	Perform	Resolvable
76	PASSWORD RESET	Management Reporting Module (MRM)	Perform	Resolvable
77	PASSWORD RESET	Old Age Security (OAS)	Perform	Resolvable
78	PASSWORD RESET	Public Accounts Production System (PAPS)	Perform	Resolvable
79	PASSWORD RESET	Online Pay (CV72) (PAY)	Perform	Resolvable
80	PASSWORD RESET	Production Control Files (PCFL)	Perform	Resolvable
81	PASSWORD RESET	Position & Classification Information System (PCIS)	Perform	Resolvable
82	PASSWORD RESET	Paper Check Reconciliation (PCR)	Perform	Resolvable
83	PASSWORD RESET	Payment Control System (PCS)	Perform	Resolvable
84	PASSWORD RESET	PWGSC Mainframe Web Application Portal (PORTAL)	Perform	Resolvable
85	PASSWORD RESET	Production Support Reporting System (PSRS)	Perform	Resolvable
86	PASSWORD RESET	RCMP Pay & Pension System (RPPS)	Perform	Resolvable
87	PASSWORD RESET	Resource Tracking & Service Level Reporting (RTSLR)	Perform	Resolvable
88	PASSWORD RESET	Standard Cheque Issue (SCI)	Perform	Resolvable
89	PASSWORD RESET	Supplier Registration Information (SRI)	Perform	Resolvable
90	PASSWORD RESET	Superannuating Management Information Reporting System (SMIRS)	Perform	Resolvable
91	PASSWORD RESET	Vendor Information Management (VIM)	Perform	Resolvable

	Type of Contact	Detail	Action	Disposition
92	MAINFRAME ACCOUNT OPERATIONS	Session Reset	Perform	Resolvable
93	ACCOUNT MODIFICATION	OTHER	ACCOUNT MODIFICATION	Non-Resolvable
94	ADHOC	Ministerial Transition	Triage, assess, synthesize, assign, Monitor	Non-Resolvable

1.3 ESD – Other (Resolvable vs. Non-resolvable)

The following Table lists the types of other interactions handled by ESD Service Desk Agents:

Table 69: ESD Contacts Handled - Other

	Type of Contact	Detail	Action	Disposition
1	INFORMATION REQUEST	Contact Information (Non-person, other service desk/help information)	Validate and provide information	Resolvable
2	INFORMATION REQUEST	Ticket Status	Respond with ticket information available	Resolvable
3	INFORMATION REQUEST	Service Inquiry	Triage, assess, synthesize, assign	Non-Resolvable
4	RE-PRIORITIZATION	Service Inquiry	Re-assessment of ticket priority would be performed	Resolvable
5	OUT OF SCOPE	Service Inquiry	Validate, confirm out of scope and resolve with notification to contact Partner Service Desk	Resolvable

2.0 EUSD Contacts Handled

The following Tables list the types of incidents/service requests handled by the End User Service Desk (EUSD). In addition, the table indicates those interactions that are expected to be resolved by the EUSD ("Resolvable Contacts") and those that are expected to be escalated to the ESD ("Non-Resolvable Contacts").

Resolvable Contacts are those incidents/service requests for which the EUSD Service Desk Agents have the necessary training and access to tools required to resolve without escalation to the ESD.

For greater clarity, Non-resolvable Contacts do not include contacts that inadvertently arrive at the EUSD but should instead have gone to another desk or organization ("Out-of-Scope Contacts"). Out-of-Scope contacts should be re-directed to the appropriate desk or organization through manual or automatic means (i.e. ACD).

These lists are subject to change at the discretion of SSC. Changes will be reviewed and agreed with the Contractor before those changes are applied.

In the instance of incidents/service requests not listed in the tables below, the Contractor is required to provide support and resolution within the performance targets keeping the customer experience intact. The Contractor is then responsible for addressing these "new" incidents/service requests with SSC in order to update the contact list as per the agreement between SSC and the Contractor.

2.1 EUSD – Incident Management (Resolvable vs. Non-resolvable)

The following Table lists the types of incidents handled by EUSD Service Desk Agents:

Table 70: EUSD Contacts Handled – Incident Management

	Type of Contact	Detail	Action	Disposition
1	TELECOM	Mobile	Triage, assess, synthesize, assign	Non-Resolvable
2	TELECOM	Fixed Line	Triage, assess, synthesize, assign	Non-Resolvable
3	NETWORK	WAN	Triage, assess, synthesize, assign	Non-Resolvable
4	NETWORK	LAN	Triage, assess, synthesize, assign	Non-Resolvable
5	NETWORK	Wi-Fi	Triage, assess, synthesize, assign	Non-Resolvable
6	MAINFRAME	Mainframe	Triage, assess, synthesize, assign	Non-Resolvable
7	SECURITY	PKI	Triage, assess, synthesize, assign	Non-Resolvable
8	SECURITY	Firewall	Triage, assess, synthesize, assign	Non-Resolvable
9	SECURITY	VPN	Triage, assess, synthesize, assign	Non-Resolvable
10	SECURITY	Remote Access	Triage, assess, synthesize, assign	Non-Resolvable
11	MIDRANGE	Midrange	Triage, assess, synthesize, assign	Non-Resolvable
12	FILE AND PRINT	File and Print	Triage, assess, synthesize, assign	Non-Resolvable
13	APPLICATIONS	Applications	Triage, assess, synthesize, assign	Non-Resolvable
14	MESSAGING	Email Legacy	Triage, assess, synthesize, assign	Non-Resolvable
15	MESSAGING	ETI	Triage, assess, synthesize, assign	Non-Resolvable
16	VIDEO CONFERENCING / TELEPRESENCE	Video Conferencing / Telepresence	Triage, assess, synthesize, assign	Non-Resolvable
17	STORAGE	Storage	Triage, assess, synthesize, assign	Non-Resolvable
18	HARDWARE	Hardware	Triage, assess, synthesize, assign	Non-Resolvable
19	FACILITIES	HVAC	Triage, assess, synthesize, assign	Non-Resolvable
20	SECURITY	Virus	Triage, assess, synthesize, assign	Non-Resolvable
21	FACILITIES	Data Centre	Triage, assess, synthesize, assign	Non-Resolvable

2.2 EUSD - Request Fulfilment (Resolvable vs. Non-resolvable)

The following Tables list the types of service requests handled by EUSD Service Desk Agents:

Table 71: EUSD Contacts Handled – Request Fulfilment [All Desks]

	Type of Contact	Detail	Action	Disposition
1	TELECOM	Mobile	Triage, assess, synthesize, assign	Non-Resolvable
2	TELECOM	Fixed Line	Triage, assess, synthesize, assign	Non-Resolvable
3	NETWORK	WAN	Triage, assess, synthesize, assign	Non-Resolvable
4	NETWORK	LAN	Triage, assess, synthesize, assign	Non-Resolvable
5	NETWORK	Wi-Fi	Triage, assess, synthesize, assign	Non-Resolvable
6	MAINFRAME	Mainframe	Triage, assess, synthesize, assign	Non-Resolvable
7	SECURITY	PKI	Triage, assess, synthesize, assign	Non-Resolvable
8	SECURITY	Firewall	Triage, assess, synthesize, assign	Non-Resolvable
9	SECURITY	VPN	Triage, assess, synthesize, assign	Non-Resolvable
10	SECURITY	Remote Access	Triage, assess, synthesize, assign	Non-Resolvable
11	SECURITY	MyKey	Triage, assess, synthesize, assign	Non-Resolvable
12	MIDRANGE	Midrange	Triage, assess, synthesize, assign	Non-Resolvable
13	FILE AND PRINT	File and Print	Triage, assess, synthesize, assign	Non-Resolvable

	Type of Contact	Detail	Action	Disposition
14	APPLICATIONS	Applications	Triage, assess, synthesize, assign	Non-Resolvable
15	APPLICATIONS	SCCM	Triage, assess, synthesize, assign	Resolvable
16	APPLICATIONS	MS Office	Triage, assess, synthesize, assign	Resolvable
17	MESSAGING	Email Legacy	Triage, assess, synthesize, assign	Non-Resolvable
18	MESSAGING	ETI	Triage, assess, synthesize, assign	Non-Resolvable
19	VIDEO CONFERENCING / TELEPRESENCE	Video Conferencing / Telepresence	Triage, assess, synthesize, assign	Non-Resolvable
20	STORAGE	Storage	Triage, assess, synthesize, assign	Non-Resolvable
21	FACILITIES	Data Centre	Triage, assess, synthesize, assign	Non-Resolvable
22	FACILITIES	HVAC	Triage, assess, synthesize, assign	Non-Resolvable
27	PASSWORD RESET	BitLocker	Perform	Resolvable
28	PASSWORD RESET	Active Directory	Perform	Resolvable
29	PASSWORD RESET	WebSuite	Perform	Resolvable
30	PASSWORD RESET	Sigma	Perform	Resolvable
31	PASSWORD RESET	Email Legacy	Perform	Resolvable
32	PASSWORD RESET	GCDOCS	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
33	PASSWORD RESET	HP Asset Manager	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
34	PASSWORD RESET	PKI/MyKey	Triage, assess, assign	Non-Resolvable
35	PASSWORD RESET	ITSSO	Triage, assess, assign	Non-Resolvable
36	HARDWARE	Mouse	Triage, assess, assign	Non-Resolvable
37	HARDWARE	Keyboard	Triage, assess, assign	Non-Resolvable
38	HARDWARE	Mobile Device	Triage, assess, assign	Non-Resolvable
39	HARDWARE	Workstation	Triage, assess, assign	Non-Resolvable
40	HARDWARE	Bluetooth	Triage, assess, assign	Resolvable
41	MOBILE DEVICE ACTIVIATION	EMDM	Perform	Resolvable
42	MOBILE DEVICE PW RESET	EMDM	Perform	Resolvable
43	MOBILE DEVICE ACTIVIATION	ETI, Legacy	Perform	Resolvable
44	MOBILE DEVICE PW RESET	ETI, Legacy	Perform	Resolvable
45	ADMINISTRATIVE PASSWORD RESET	Administrative Password Reset	Triage, assess, assign	Non-Resolvable
46	PRINT QUE JOB MANAGEMENT	Print Que Job Management	Triage, assess, assign	Non-Resolvable

Table 72: EUSD Contacts Handled – Request Fulfilment [PSPC Desk]

	Type of Contact	Detail	Action	Disposition
1	PASSWORD RESET	Novell	Perform	Resolvable
2	PASSWORD RESET	CITRIX	Perform	Resolvable
3	PASSWORD RESET	CITRIX Admin	Triage, assess, assign	Non-Resolvable
4	PASSWORD RESET	Voicemail	Triage, assess, assign	Non-Resolvable
5	PASSWORD RESET	PeopleSoft	Triage, assess, assign	Non-Resolvable
6	PASSWORD RESET	Secure USB Passwords	Perform	Resolvable

	Type of Contact	Detail	Action	Disposition
7	PASSWORD RESET	OSSRO FOR Validators - CA's - SDA's	Perform	Resolvable
8	PASSWORD RESET	AMS	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
9	PASSWORD RESET	WinOrg	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
10	PASSWORD RESET	ABE-Vim-MERX	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
11	PASSWORD RESET	ARTS	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
12	PASSWORD RESET	OLISS	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
13	PASSWORD RESET	ELF	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
14	PASSWORD RESET	E-Purchasing	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
15	PASSWORD RESET	RPMS (Real Property Management Sys)	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
16	PASSWORD RESET	RightFax	Triage, assess, assign	Non-Resolvable
17	PASSWORD RESET	Reset Printer Passwords	Triage, assess, assign	Non-Resolvable
18	PASSWORD RESET	LASERFICHE	Triage, assess, assign	Non-Resolvable
19	PASSWORD RESET	KEYENTRY 3	Triage, assess, assign	Non-Resolvable
20	PASSWORD RESET	ITSR-ITSO	Triage, assess, assign	Non-Resolvable
21	PASSWORD RESET	ISS	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
22	PASSWORD RESET	ISIS	Triage, Assess, Provide Alternate Helpdesk Details	Resolvable
23	PASSWORD RESET	Clearquest	Triage, assess, assign	Non-Resolvable

Table 73: EUSD Contacts Handled – Request Fulfilment [SSC Desk]

	Type of Contact	Detail	Action	Disposition
1	**PASSWORD RESET**	**Novell**	**Perform**	**Resolvable**
2	**PASSWORD RESET**	**CITRIX**	**Perform**	**Resolvable**
3	**PASSWORD RESET**	**CITRIX Admin**	**Triage, assess, assign**	**Non-Resolvable**
4	**PASSWORD RESET**	**Voicemail**	**Triage, assess, assign**	**Non-Resolvable**
5	**PASSWORD RESET**	**PeopleSoft**	**Triage, assess, assign**	**Non-Resolvable**
6	**PASSWORD RESET**	**Secure USB Passwords**	**Perform**	**Resolvable**
7	**PASSWORD RESET**	**Email @Canada (ETI)**	**Perform**	**Resolvable**
8	**PASSWORD RESET**	**CIMS-CNSS-IPS**	**Triage, Assess, Provide Alternate Helpdesk Details**	**Resolvable**
9	**PASSWORD RESET**	**Appgate**	**Triage, Assess, Provide Alternate Helpdesk Details**	**Resolvable**
10	**PASSWORD RESET**	**Confluence**	**Triage, Assess, Provide Alternate Helpdesk Details**	**Resolvable**

Table 74: EUSD Contacts Handled – Request Fulfilment [HC Desk]

	Type of Contact	Detail	Action	Disposition
1	PASSWORD RESET	Novell	Perform	Resolvable
2	PASSWORD RESET	Email @Canada (ETI)	Perform	Resolvable

Table 75: EUSD Contacts Handled – Request Fulfilment [INFC Desk]

	Type of Contact	Detail	Action	Disposition
1	PASSWORD RESET	Email @Canada (ETI)	Perform	Resolvable

Table 76: EUSD Contacts Handled – Request Fulfilment [CSPS Desk]

	Type of Contact	Detail	Action	Disposition
1	PASSWORD RESET	Novell	Perform	Resolvable
2	PASSWORD RESET	Email @Canada (ETI)	Perform	Resolvable

2.3 EUSD – Other (Resolvable vs. Non-resolvable)

The following Tables list the types of other interactions handled by EUSD Service Desk Agents:

Table 77: EUSD Contacts Handled – Other

	Type of Contact	Detail	Action	Disposition
1	INFORMATION REQUEST	Contact Information	Perform	Resolvable
2	INFORMATION REQUEST	Ticket Status	Perform	Resolvable
3	INFORMATION REQUEST	Service Inquiry	Perform	Resolvable

3.0 ESD Resolver Groups

The ESD dispatches to the following Resolver Groups at the time of the creation of this document:

ESD Resolver Groups.xlsx

Schedule A 14 – Service Desk Workload Baseline

Shared Services Canada

Schedule A 14 – Service Desk Workload Baseline

Table of Contents

List of Tables

List of Figures

Schedule A 14 – Service Desk Workload Baseline

This Schedule describes current contact volumes associated with the Service Desk Services described in **Schedule A 1 – Service Desk Services**.

1.0 Enterprise Service Desk (ESD)

This section provides historical contact volumes for the following elements of the ESD:

i. ESD Supported Partners / ESD Supported Non-Partner Clients;

ii. ESD Supported Partners: Partially On-Boarded (Formerly Government Operations Portfolio);

iii. ESD Customers: After Hours Support for Partner Service Desk(s); and

iv. ESD Total All Customers.

1.1 ESD Supported Partners / ESD Supported Non-Partner Clients

This section provides historical contact volumes for the available intake channels:

Table 78: Contact Volumes for ESD Supported Partners / ESD Supported Non-Partner Clients

		Phone Calls Answered[1]	ESD E-mail[2]	E-mail Listener[3]	Self-service Portal[4]	TOTAL
2019	May	2,709	7,943	9,027	2,862	22,541
	June	2,605	13,507	7,493	2,540	26,145
	July	3,163	6,488	8,131	3,090	20,872
	August	2,542	5,441	6,941	2,727	17,651
	September	2,634	6,827	7,527	3,012	20,000
	October	2,827	7,731	7,802	3,071	21,431
	November	2,806	7,806	5,954	2,827	19,393
	December	2,326	5,994	4,980	2,577	15,877
2020	January	3,016	7,607	6,073	2,776	19,472
	February	2,854	7,170	5,478	2,566	18,068
	March	2,756	7,294	5,433	2,214	17,697
	April	2,050	5,396	3,672	1,395	12,513

SOURCE: ***Enterprise Service Desk Monthly Report: April 2020***

Phone to ESD (1-855-830-7782 option 1) / Mobile Travel Devices (1-416-861-8594)

1. ESD E-mail (SSC.enterpriseservicedesk-bureaudeservicedentreprise.SPC@canada.ca) to ESD ITSM Tool
2. E-mail Listener operating as a bridge between Partner ITSM Tool and ESD ITSM Tool
3. Self-Service Portal to ESD ITSM Tool
4. Service Catalogue

1.2 ESD Supported Partners: Partially On-Boarded (Formerly Government Operations Portfolio)

This section provides historical contact volumes for the available intake channels:

Table 79: Contact Volumes for ESD Supported Partners: Partially On-Boarded

		Phone Calls Answered[1]	NSD E-mail[2]	E-mail Listener	Self-service Portal	TOTAL
2019	May	992	6,011	-	-	7,003
	June	984	5,527	-	-	6,511
	July	1,097	5,638	-	-	6,735
	August	854	4,906	-	-	5,760
	September	977	4,693	-	-	5,670
	October	806	5,257	-	-	6,063
	November	830	5,120	-	-	5,950
	December	643	4,355	-	-	4,998
2020	January	861	4,615	-	-	5,476
	February	895	4,282	-	-	5,177
	March	986	4,113	-	-	5,099
	April	893	3,021	-	-	3,914

SOURCE: ***Enterprise Service Desk Monthly Report: April 2020***

1. Phone to ESD (1-855-830-7782 option 1) / Mobile Travel Devices (1-416-861-8594)
2. National Service Desk E-mail (SSC.nationalservicedesk-bureaudeservicenational.SPC@canada.ca) to InfoWeb Tool

1.3 ESD Customers: After Hours Support for Partner Service Desk(s)

This section provides historical contact volumes for the available intake channels:

Table 80: Contact Volumes for ESD After Hours Customers

		Phone Calls Answered[1]	ESD E-mail	E-mail Listener	Self-service Portal	TOTAL
2019	May	179	-	-	-	179
	June	174	-	-	-	174
	July	252	-	-	-	252
	August	157	-	-	-	157
	September	216	-	-	-	216
	October	178	-	-	-	178
	November	136	-	-	-	136
	December	68	-	-	-	68
2020	January	122	-	-	-	122
	February	139	-	-	-	139
	March	364	-	-	-	364
	April	160	-	-	-	160

SOURCE: ***Enterprise Service Desk Monthly Report: April 2020***

Phone: TC/Assist (613-991-8908).

1.4 ESD Total All Customers

This section provides historical contact volumes for the available intake channels:

Table 81: Total Contact Volumes for All ESD Custmoers

		Phone Calls Answered	ESD E-mail	E-mail Listener	Self-service Portal	TOTAL
2019	May	3,880	13,954	9,027	2,862	29,723
	June	3,763	19,034	7,493	2,540	32,830
	July	4,512	12,126	8,131	3,090	27,859
	August	3,553	10,347	6,941	2,727	23,568
	September	3,827	11,520	7,527	3,012	25,886
	October	3,811	12,988	7,802	3,071	27,672
	November	3,772	12,926	5,954	2,827	25,479
	December	3,037	10,349	4,980	2,577	20,943
2020	January	3,999	12,222	6,073	2,776	25,070
	February	3,888	11,452	5,478	2,566	23,384
	March	4,106	11,407	5,433	2,214	23,160
	April	3,103	8,417	3,672	1,395	16,587

SOURCE: ***Enterprise Service Desk Monthly Report: April 2020***

2.0 End User Service Desk (EUSD)

This section provides historical contact volumes for the following elements of the EUSD:

i. Public Services and Procurement Canada;
ii. Health Canada (Public Health Agency of Canada and Patented Medicine Prices Review Board);
iii. Shared Services Canada;
iv. Canada School of Public Service;
v. Infrastructure Canada; and
vi. EUSD Total All Customers.

2.1 Public Service and Procurement Canada

This section provides historical contact volumes for the available intake channels:

Table 82: Contact Volumes for Public Service and Procurement Canada

		Phone Calls Answered[1]	Emails Processed	Self-service Portal[2]	Total
2019	May	12,842	-	4,835	17,677
	June	11,682	-	3,824	15,506
	July	11,704	-	3,675	15,379
	August	10,065	-	3,415	13,480
	September	9,809	-	3,558	13,367
	October	9,435	-	3,423	12,858
	November	9,330	-	2,943	12,273
	December	8,366	-	2,685	11,051
2020	January	10,810	-	3,283	14,093
	February	9,655	-	2,883	12,538
	March	12,004	-	1,970	13,974
	April	10,715	-	1,018	11,733

SOURCE: ***PSPC Service Desk Monthly Report: April 2020***

1. Various (see Table 2-2 EUSD Contact Channels of **Schedule A 12 – Customers Supported**).
2. Office System Service Request Online (OSSRO).

2.2 Health Canada (Public Health Agency of Canada and Patented Medicine Prices Review Board)

This section provides historical contact volumes for the available intake channels:

Table 83: Contact Volumes for Health Canada

		Phone Calls Answered[1]	Emails Processed[2]	Self-service Portal	Total
2019	May	8,114	4,887	-	13,001
	June	6,654	4,105	-	10,759
	July	6,762	4,675	-	11,437
	August	5,772	3,189	-	8,961
	September	7,589	4,093	-	11,682
	October	7,714	4,361	-	12,075
	November	7,982	4,425	-	12,407
	December	6,642	3,177	-	9,819
2020	January	9,651	4,731	-	14,382
	February	7,194	3,905	-	11,099
	March	10,396	3,640	-	14,036
	April	7,386	2,826	-	10,212

SOURCE: ***HC Service Desk Monthly Report: April 2020***

1. Phone to EUSD (1-800-416-0358); Direct Local (613-954-8718).
2. HC E-mail (hc.nationalservicedesk-bureaudeservicenational.sc@canada.ca) to EUSD ITSM Tool.

2.3 Shared Services Canada

This section provides historical contact volumes for the available intake channels:

Table 84: Contact Volumes for Shared Services Canada

		Phone Calls Answered[1]	Emails Processed	Self-service Portal[2]	Total
2019	May	5,797	-	4,159	9,956
	June	5,732	-	3,248	8,980
	July	6,187	-	3,404	9,591
	August	5,046	-	3,204	8,250
	September	5,213	-	3,278	8,491
	October	5,495	-	4,017	9,512
	November	5,494	-	3,551	9,045
	December	4,293	-	2,752	7,045
2020	January	5,377	-	3,519	8,896
	February	5,739	-	3,302	9,041
	March	6,126	-	2,811	8,937
	April	4,251	-	2,987	7,238

SOURCE: ***SSC Service Desk Monthly Report: April 2020***

1. Phone to EUSD (1-855-591-0550); External Transfer (1-855-830-7782) after hours.
2. Government of Canada Service Express (GCSX).

2.4 Canada School of Public Service

This section provides historical contact volumes for the available intake channels:

Table 85: Contact Volumes for Canada School of Public Service

		Phone Calls Answered[1]	Emails Processed[2]	Self-service Portal	Total
2019	May	1,139	465	-	1,604
	June	977	453	-	1,430
	July	750	401	-	1,151
	August	658	272	-	930
	September	781	411	-	1,192
	October	681	467	-	1,148
	November	519	347	-	866
	December	460	279	-	739
2020	January	695	348	-	1,043
	February	548	286	-	834
	March	550	196	-	746
	April	485	126	-	611

SOURCE: ***CSPS Service Desk Monthly Report: April 2020***

1. Phone to EUSD (1-833-228-9068); Direct Local (613-943-6236); External Transfer (1-855-830-7782) after hours.
2. CSPS E-mail (csps.itservicedeskbureaudeserviceti.efpc@canada.ca) to EUSD ITSM Tool.

2.5 Infrastructure Canada

This section provides historical contact volumes for the available intake channels:

Table 86: Contact Volumes for Infrastructure Canada

		Phone Calls Answered[1]	Emails Processed[2]	Self-service Portal	Total
2019	May	258	459	-	717
	June	185	371	-	556
	July	157	484	-	641
	August	106	350	-	456
	September	140	397	-	537
	October	151	389	-	540
	November	89	319	-	408
	December	88	275	-	363
2020	January	128	485	-	613
	February	116	513	-	629
	March	167	341	-	508
	April	153	113	-	266

SOURCE: ***INFC Service Desk Monthly Report: April 2020***

1. Phone to EUSD (1-833-228-9069); Direct Local (613-941-2427); External Transfer (1-855-830-7782) after hours.
2. INFC E-mail (infc.itservices-servicesti.infc@canada.ca) to EUSD ITSM Tool.

2.6 EUSD Total All Customers

This section provides historical contact volumes for the available intake channels:

Table 87: Contact Volumes for all EUSD Customers

		Phone Calls Answered	Emails Processed	Self-service Portal	Total
2019	May	28,150	5,811	8,994	42,955
	June	25,230	4,929	7,072	37,231
	July	25,560	5,560	7,079	38,199
	August	21,647	3,811	6,619	32,077
	September	23,532	4,901	6,836	35,269
	October	23,476	5,217	7,440	36,133
	November	23,414	5,091	6,494	34,999
	December	19,849	3,731	5,437	29,017
2020	January	26,661	5,564	6,802	39,027
	February	23,252	4,704	6,185	34,141
	March	29,243	4,177	4,781	38,201
	April	22,990	3,065	4,005	30,060

SOURCE: ***PSPC/HC/SSC/CSPS/INFC Service Desk Monthly Reports: April 2020***

3.0 Additional Data

In addition to the contact volumes by intake channel provided in this schedule, SSC will make supplemental volumetric information available for the ESD and for each of the service desks within the EUSD. This information will be made available to bid proponents during the RFP posting period.

Schedule A 15 – Privacy

Shared Services Canada

Schedule A 15 – Privacy

Table of Contents

Schedule A 15 – Privacy

This Schedule describes the responsibilities of the Contractor with respect to privacy and the protection of personal information associated with the provision of Service Desk Services described **in Schedule A 1 – Service Desk Services**.

Note: The following clauses will apply in the event that personal information is collected, accessed and/or handled by the service stakeholders/Contractors.

1.0 Service Management Guide

The Contractor must provide a service management guide within sixty (60) Federal Government Working Days (FGWD) after Contract award to SSC for approval. The guide, provided for the Enterprise Vulnerability Management Solution, shall include:

- Privacy breach process; and
- Security breach process.

2.0 Privacy Breach Report

The Contractor must provide a privacy breach report to SSC, by reporting period specified by SSC, on privacy breaches that includes:

- Number of privacy Incidents;
- Number of privacy investigations completed; and
- Average/highest response time to privacy Incidents.

3.0 Privacy Management Plan

The privacy management plan demonstrates that the Contractor can meet the requirements of the Contract and provide assurance of their ability to manage Personal Information and Records in accordance with the statutory obligations.

The Contractor must provide a draft privacy management plan within sixty (60) Federal Government Working Days (FGWD) after Contract award to SSC for approval. SSC reserves the right to request changes to the privacy management plan in order to ensure that privacy is being properly managed by the Contractor.

The Contractor must provide SSC with an update to its privacy management plan within twenty (20) Federal Government Working Days of a request by SSC.

The privacy management plan must specifically describe the following items in detail:

(a) Contractor's privacy protection strategies and detail exactly how the Personal Information will be treated over its life cycle;

(b) How the Personal Information will be collected, used, retained, disclosed and disposed only for the purposes of the Work specified in the Contract;

(c) How the Personal Information and Records will be accessible only to authorized individuals (on a need-to-know basis) for the purposes of the Work specified in the Contract;

(d) The privacy breach protocol, and details on how any privacy breaches will be handled;

(e) How the Contractor intends to ensure that Canadian Privacy requirements, as outlined in the Privacy Act, the Access to Information Act and Library and Archives of Canada Act, will be met throughout the performance of the Work and for the duration of the Contract;

(f) Any new measures the Contractor intends to implement in order to safeguard the Personal Information and the Records in accordance with their security classification;

(g) How the Contractor intends to ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification; and

(h) Describe how the Contractor intends to ensure that their staff is trained on privacy and privacy related principals.

4.0 Privacy Impact Assessment

The Contractor must assist SSC in creating the privacy impact assessment in accordance with the TBS Directive on privacy impact assessment (http://www.tbs-sct.gc.ca/pol/docengaspx?id=18308&section=text#cha1) by providing the following information within twenty (20) Federal Government Working Days of a request by SSC:

(a) Business processes, data flows and procedures for the collection, transmission, processing, storage, disposal and access to information including Personal Information;

(b) A list of the Personal Information used by the Contractor in connection with the Work and the purpose of each Personal Information item;

(c) How the Personal Information is shared and with whom;

(d) A list of all locations where hard copies of Personal Information are stored;

(e) A list of all locations where Personal Information in machine-readable format is stored (e.g., the location where any server housing a database including any Personal Information is located), including back-ups;

(f) A list of all measures being taken by the Contractor to secure the Personal Information and the Records beyond those required by the Contract; and

(g) Any privacy-specific security requirements or recommendations that need to be addressed.

Schedule A 16 – Professional Services

Shared Services Canada

Schedule A 16 – Professional Services

Table of Contents

Schedule A 16 – Professional Services

1.0 Professional Services Overview

SSC may require the services of additional resources from the Contractor on an "as and when requested" basis to assist in addressing unforeseen related requirements (e.g. resolve a catastrophic event, support emergency or crisis situations, assist in planning a migration to a new system platform).

Services required will be defined through the Task Authorization process, including language requirements, level of effort and location of work.

The Contractor must provide resources to SSC, in accordance with a validly issued Task Authorization, in the following job categories or equivalent:

a) Client Executive;
b) Service Delivery Manager;
c) Business Analyst;
d) Project Manager;
e) Business Continuity/Disaster Recovery Specialist; and
f) Service Desk Support Agent.

1.1 Client Executive

The role and responsibilities of the Client Executive will include, but are not limited to, the following:

- Act as the primary Relationship Manager between the Contractor and SSC, ensure the overall optimum health of all in-scope services and that all SOW requirements are met;
- Participate in the resolution of escalated Problems, Disputes, Incidents, and Service and Contract Changes;
- Work with SSC to address relevant high-level issues and proposing innovations and process improvements related to the Contract services in support of SSC strategic business transformation;
- Ensure that all personnel designated with a Key Role in the SOW are knowledgeable about SSC's Service Lines, as well as the Contractor's and its subcontractors' own products and services;
- Liaise with SSC and Contractor internal service groups and formulate internal resourcing strategy to fulfill the demand pipeline to address resourcing needs; and
- Proactively monitor overall progress and report at regular intervals to key stakeholders, resolving issues and initiating corrective action, as appropriate, and in accordance with the situation requirements. Proactively escalate to the appropriate stakeholders, as necessary.

1.2 Service Delivery Manager

The role and responsibilities of the Service Delivery Manager will include, but are not limited to, the following:

- Act as the Manager for services provided to SSC, ensure the overall optimum health of all in-scope services and that all service requirements are met;
- Coordinate the resolution of escalated Problems, Disputes, Incidents, and Service and Contract Changes;
- Ensure appropriate allocation and coordination of resources to meet service requirements;
- Ensure that all front-line personnel are knowledgeable about SSC, the service environment, processes and procedures;
- Be knowledgeable about SSC's Service Lines, and the Contractor's and its Subcontractors' own products and services;
- Liaise with SSC to provide strategic guidance and recommendations on IT Service Management business;
- Ensure demand and related requirements are understood and factored into capacity plans;

- Provide reporting and status of the service desk as well as relay operational changes needed to be implemented by the service desk; and
- Provide ongoing support activities associated with emergency or crisis situations.

1.3 Business Analyst

The role and responsibilities of the Business Analyst will include, but are not limited to, the following:

- Develop and document statements of requirements for considered alternatives;
- Perform business analyses of functional requirements to identify information, procedures, and decision flows;
- Evaluate existing procedures and methods, identify and document items such as database content, structure, application subsystems;
- Define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems;
- Develop a testing strategy and plan;
- Establish acceptance test criteria with client;
- Support and use the selected departmental methodologies; and
- Create a project schedule and produce and maintain a requirements traceability matrix.

1.4 Project Manager

The role and responsibilities of the Project Manager will include, but are not limited to, the following:

- Manage several Project Managers, each responsible for an element of the project and its associated project team;
- Manage the project during the development, implementation and operations startup by ensuring that resources are made available and that the project is developed and is fully operational within previously agreed time, cost and performance parameters;
- Formulate statements of problems; establishes procedures for the development and implementation of significant, new or modified project elements to solve these problems, and obtains approval thereof;
- Define and document the objectives for the project; determine budgetary requirements, the composition, roles and responsibilities and terms of reference for the project team;
- Report progress of the project on an ongoing basis and at scheduled points in the life cycle;
- Meets in conference with stakeholders and other project managers and states problems in a form capable of being solved;
- Prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools; and
- Project sign-off.

1.5 Business Continuity/Disaster Recovery Specialist

The role and responsibilities of the Business Continuity/Disaster Recovery Specialist will include, but are not limited to, the following:

- Develop and implement business and technology continuity plans;
- Develop technology and business continuity and disruption recovery strategies;
- Develop crisis communication planning strategies;
- Identify past and potential impact resulting from disruptions;
- Develop techniques to identify and evaluate potential disruptions;
- Develop and implement backup, replication and redundancy strategies as required;
- Develop awareness, training, and communication programs with both internal staff and other stakeholders;

- Establish coordination activities with internal and external stakeholders and establish actual and potential dependencies; and
- Develop and implement monitoring activities and performance management.

1.6 Service Desk Support Agent (Bilingual English and French)

The role and responsibilities of the Service Desk Support Agent will include, but are not limited to, the following:

- Answer calls, performs basic troubleshooting, attempts first call resolution and respond appropriately to user requests and problems;
- Perform initial problem analysis and triage problem to the appropriate contacts as necessary;
- Maintain liaison with end-users and technical staff to communicate the status of problem resolution to end-users; log and track requests for assistance;
- Develop, implement, and/or participate in the preparation of procedure manuals and documentation for help desk use;
- Develop, implement, and/or participate in the distribution of network related information to users to include information such as help desk procedures and network handbooks;
- Participate in the development of a comprehensive training plan for help desk procedures; assist in training personnel providing backup coverage;
- Participate in on-site installations of network systems for users; and
- Perform other related duties incidental to the work described herein.

2.0 Location of Work and Travel

The Contractor may be required to participate in meetings with SSC in the National Capital Region either by videoconference, teleconference or in person. The location of the work will be in Canada, as specified in the Task Authorization. Work may be conducted on-site or off-site, as specified in the Task Authorization. All travel costs and living expenses are the responsibility of the Contractor.

3.0 Language Requirement

The Contractor must provide the required services in the English language, spoken and written, with the exception of the following:

- The Service Desk Support Agent must be fully bilingual.

The language requirement, including documentation, will be specified in the related Task Authorization.

Schedule B 1 – Pricing Provisions

Shared Services Canada

Schedule B 1 – Pricing Provisions

Table of Contents

Schedule B 1 – Pricing Provisions

1.0 Definitions

"Additional Resource Charges" or "ARCs"
Means an additional resource charge, as calculated in accordance with this **Schedule B 1 – Pricing Provisions**.

"Additional Resource Charges Unit Rate" or "ARC Unit Rate"
Means, with respect to a Base Service to be charged using a Monthly Variable Service Cost, the unit dollar charge rate for certain excess Service Volumes experienced by Shared Services Canada (SSC) during a Measurement Period, as set forth in Section 2.2 of **ANNEX B – BASIS OF PAYMENT**.

"Base Services"
Means each ongoing, recurring Service provided by the Contractor to SSC pursuant to the Statement of Work as set forth in Annex A - Statement of Work.

"Dead Band"
Means the percentage variance of Service Volumes above or below the Monthly Baseline Service Volumes, and within which ARCs (Additional Resource Charges) and RRCs (Reduced Resource Charges) are not applicable. This is set at five percent (5%).

"Final Services Commencement Date"
This is the date at which SSC has approved the service(s) to be deployed, as per Section 3.1.6 of **Schedule A 3 – Transition Services**, Table 46, item 6.19.

"Measurement Period"
Means the immediately preceding three (3) calendar months.

"Monthly Baseline Service Volume"
Means the Monthly Baseline Service Volumes established in Section 2.1.1 of **ANNEX B – BASIS OF PAYMENT**.

"Actual Service Volume"
Means Qualifying Contacts for the Enterprise Service Desk (ESD) and End User Service Desk (EUSD) in a month.

"Qualifying ESD Contacts"
Means legitimate contacts for Service Requests, Incident Reports and Change Management Requests made by Partner Service Desk Agents to the ESD via the following channels:

iv. Telephone
v. Email
vi. Email Listener

"Qualifying EUSD Contacts"
Means legitimate contacts for Service Requests, and Incident Reports made by End-User Service Desk Agents to the EUSD via the following channels:

iii. Telephone
iv. Email

"Reduced Resource Charges Unit Rate" or "RRC Unit Rate"
Means, with respect to a Base Service to be charged using a Monthly Variable Service Cost, the unit dollar credit rate for certain Service Volumes not experienced by SSC during a Measurement Period, as set forth in Section 2.2 of **ANNEX B – BASIS OF PAYMENT**.

"Reduced Resource Credits" or "RRCs"
Means a reduced resource credit, as calculated in accordance with this **Schedule B 1 – Pricing Provisions**.

"Monthly Variable Service Costs"
Means the periodic Cost for the volume of each Base Service performed by the Contractor and consumed by SSC in the amount of the Monthly Baseline Service Volume for such Base Service, for a particular month.

"Upset Limit"
Means the (+/-) range for which consistent Actual Service Volumes experienced outside the range over the Measurement Period will trigger a re-establishment of the Monthly Baseline Service Volume, Variable Service Unit Cost and Variable Service Cost Adjustments (ARC and Reduce RRC).

"Variable Service Cost Adjustment"
Means the cost adjustment to be applied when the Actual Service Volume for the Measurement Period is greater or less than the Dead Band (+/ 5% of Monthly Baseline Service Volume) for each month of the Measurement Period.

2.0 Calculation of Costs

2.1 Transition Service Cost

The cost of transitioning the Service Desk Service shall be invoiced to SSC in accordance with the Transition Milestone Payments set forth in Section 1 of **ANNEX B – BASIS OF PAYMENT**.

For contacts handled by the Contractor during the ramp-up of services prior to the Final Service Commencement date, the Contractor shall be paid the product of actual contacts handled in a given month and the applicable Year 1 Monthly Variable Service Unit Cost (see **ANNEX B – BASIS OF PAYMENT**). For greater certainty, the Monthly Baseline Service Volume and Variable Service Cost Adjustments will not apply until after the Final Service Commencement Date.

2.2 On-going Service Costs

This Section details the On-going Service Cost for the Enterprise Service Desk (ESD) and End User Service Desk (EUSD) services. The On-going Service Cost will be comprised of the following:

i. Monthly Variable Service Cost
ii. Variable Service Cost Adjustment

2.2.1 Monthly Variable Service Cost

The Variable Service Cost for the ESD and EUSD Base Services shall be invoiced to SSC on a monthly basis and is set forth in **ANNEX B – BASIS OF PAYMENT**.

2.2.2 Variable Service Cost Adjustments

This Section describes how Variable Service Costs Adjustments will be applied. This Section shall be effective with respect to a Base Service beginning on the first day of the first calendar quarter following the Final Services Commencement Date with respect to such Service, but in no event prior to the Final Services Commencement Date. Unless otherwise set forth in the Statement of Work, the Monthly Variable Service Costs (together with the adjustments made pursuant to this Section are the sole mechanism for increasing (and decreasing) the Contractor's Costs to reflect monthly increases (or decreases) in the volume of each Base Service consumed by SSC.

2.2.3 Additional Resource Charge (ARC)

In certain circumstances where the Service Volume experienced by SSC exceeds the Monthly Baseline Service Volume by more than the Dead Band, the Contractor shall invoice SSC for an ARC.

2.2.3.1 Measurement

At the beginning of each calendar quarter, the Contractor will compare the actual monthly Service Volumes experienced by SSC in the Measurement Period (with respect to each Base Service to be charged using a Monthly Variable Service Cost) against the Monthly Baseline Service Volume for such Base Service, and provide the data to SSC. If, with respect to such a Base Service, in each of the three (3) calendar months in the Measurement Period, the actual Service Volume experienced by SSC with respect to such Base Service was greater than the Monthly Baseline Service Volume for such Base Service by more than the Dead Band, then the Contractor shall Invoice SSC for an ARC with respect to such Base Service, as described below.

2.2.3.2 Calculation

With respect to any Base Service to be charged using a Monthly Variable Service Cost, ARCs shall be calculated as follows:

i. **ARC volume fluctuation month 1**
Actual Service Volume experienced by SSC in the first calendar month of the Measurement Period – (Monthly Baseline Service Volume * 1.05).

ii. **ARC volume fluctuation month 2**
Actual Service Volume experienced by SSC in the second calendar month of the Measurement Period – (Monthly Baseline Service Volume * 1.05).

iii. **ARC volume fluctuation month 3**
Actual Service Volume experienced by SSC in the third calendar month of the Measurement Period – (Monthly Baseline Service Volume * 1.05).

iv. **ARC for Measurement Period**
ARC Unit Rate for such Base Services * (ARC volume fluctuation month 1 + ARC volume fluctuation month 2 + ARC volume fluctuation month 3).

For avoidance of doubt, ARC payments for a given calendar month will not be made more than once with respect to any particular Base Service.

2.2.3.3 Examples

The examples below demonstrate how the ARC calculation would be determined.

a) **Example 1 -** Actual Service Volumes exceed the Dead Ban Upper Limit in three (3) consecutive months

Month	Monthly Baseline Service Volume (MBSV)	Dead Band Upper Limit (MBSV x 105%)	Actual Service Volume	ARC Volume Fluctuation
1	36,000	37,800	38,300	500
2	36,000	37,800	39,300	1,500
3	36,000	37,800	38,800	1,000
Cumulative Volume Fluctuation for Measurement Period				3,000
ARC Unit Rate (example)				$20
ARC for Measurement Period				$60,000

In this Example, an ARC is payable since Actual Service Volumes exceeded the Monthly Baseline Service Volume by more than 5% in three consecutive months.

b) **Example 2 -** Actual Service Volumes exceed the Dead Ban Upper Limit in four (4) consecutive months

Month	Monthly Baseline Service Volume (MBSV)	Dead Band Upper Limit (MBSV x 105%)	Actual Service Volume	ARC Volume Fluctuation
1	36,000	37,800	38,300	500
2	36,000	37,800	39,300	1,500
3	36,000	37,800	39,800	2,000
4	36,000	37,800	38,550	750
Cumulative Volume Fluctuation for Fourth Consecutive Month				750
ARC Unit Rate (example)				$20
ARC for Fourth Consecutive Month				$15,000

In this example, an ARC is payable in respect of Month 4 since Actual Service Volumes exceeded the Monthly Baseline Service volume by more than 5% in three consecutive months; however, charges for Month 2 and Month 3 would have already been made and the charge is limited to the ARC Volume Fluctuation for Month 4.

c) **Example 3 -** Actual Service Volumes exceed the Dead Ban Upper Limit in two (2) consecutive months

Month	Monthly Baseline Service Volume (MBSV)	Dead Band Upper Limit (MBSV x 105%)	Actual Service Volume	ARC Volume Fluctuation
1	36,000	37,800	38,300	500
2	36,000	37,800	39,300	1,500
3	36,000	37,800	36,500	nil
Cumulative Volume Fluctuation for Measurement Period				nil
ARC Unit Rate (example)				$20
ARC for Measurement Period				nil

In this example, no ARC would be payable because the Actual Service Volume experienced in each month of the Measurement Period did not exceed the Monthly Baseline Service Volume by more than the Dead Band (i.e., the Actual Service Volume experienced in the third month did not exceed the Monthly Baseline Service Volume by more than five percent (5%)).

2.2.4 Reduce Resource Credit (RRC)

2.2.4.1 Measurement

At the beginning of each calendar quarter, the Contractor will compare the Actual Service Volumes experienced by SSC in the Measurement Period with respect to each Base Service to be charged using a Monthly Variable Service Cost against the current Monthly Baseline Service Volume for such Base Service, and provide the data to SSC. If, with respect to such a Base Service, in each of the three (3) calendar months in the Measurement Period, the Actual Service Volume experienced by SSC with respect to such Base Service was less than the Monthly Baseline Service Volume for such Base Service by more than the Dead Band, then the Contractor will pay or credit to SSC a RRC with respect to such Base Service, as described below.

2.2.4.2 Calculation

With respect to any Base Service to be charged using a Monthly Variable Service Cost, RRCs shall be calculated as follows:

i. **RRC volume fluctuation month 1**
(Monthly Baseline Service Volume * .95) – Actual Service Volume experienced by SSC in the first calendar month of the Measurement Period.

ii. **RRC volume fluctuation month 2**
(Monthly Baseline Service Volume * .95) – Actual Service Volume experienced by SSC in the second calendar month of the Measurement Period.

iii. **RRC volume fluctuation month 3**
(Monthly Baseline Service Volume * .95) – Actual Service Volume experienced by SSC in the third calendar month of the Measurement Period.

iv. **RRC for Measurement Period**
RRC Unit Rate for such Base Services * (RRC volume fluctuation month 1 + RRC volume fluctuation month 2 + RRC volume fluctuation month 3).

For avoidance of doubt, RRC payments or credits for a particular calendar month will not be made more than once with respect to any particular Base Service.

2.2.4.3 Examples

The examples below demonstrates how the RRC calculation would be determined.

a) **Example 1 -** Actual Service Volumes below the Dead Ban Lower Limit in three (3) consecutive months

Month	Monthly Baseline Service Volume (MBSV)	Dead Band Lower Limit (MBSV x 95%)	Actual Service Volume	RRC Volume Fluctuation
1	36,000	34,200	32,700	(1,500)
2	36,000	34,200	33,700	(500)
3	36,000	34,200	32,200	(2,000)
Cumulative Volume Fluctuation for Measurement Period				(4,000)
RRC Unit Rate (example)				$20
RRC for Measurement Period				($80,000)

In this Example, an RRC is creditable since Actual Service Volumes were below the Monthly Baseline Service Volume by more than 5% in three consecutive months.

b) **Example 2 -** Actual Service Volumes below the Dead Ban Lower Limit in four (4) consecutive months

Month	Monthly Baseline Service Volume (MBSV)	Dead Band Lower Limit (MBSV x 105%)	Actual Service Volume	RRC Volume Fluctuation
1	36,000	34,200	32,700	(1,500)
2	36,000	34,200	33,700	(500)
3	36,000	34,200	32,200	(2,000)
4	36,000	34,200	33,200	(1,000)
Cumulative Volume Fluctuation for Fourth Consecutive Month				(1,000)
RRC Unit Rate (example)				$20
RRC for Fourth Consecutive Month				($20,000)

In this example, an RRC is creditable in respect of Month 4 since Actual Service Volumes were below the Monthly Baseline Service volume by more than 5% in three consecutive months; however, credits for Month 2 and Month 3 would have already been made and the charge is limited to the RRC Volume Fluctuation for Month 4.

c) **Example 3 -** Actual Service Volumes below the Dead Band Lower Limit in two (2) consecutive months

Month	Monthly Baseline Service Volume (MBSV)	Dead Band Upper Limit (MBSV x 105%)	Actual Service Volume	RRC Volume Fluctuation
1	36,000	34,200	32,700	(1,500)
2	36,000	34,200	33,700	(500)
3	36,000	34,200	34,500	Nil
Cumulative Volume Fluctuation for Measurement Period				nil
RRC Unit Rate (example)				$20
RRC for Measurement Period				nil

In this example, no RRC would be creditable because the Actual Service Volumes experienced in each month of the Measurement Period were not less than the Monthly Baseline Service Volume by more than the Dead Band (i.e., the Actual Service Volume experienced in the third month was not less than the Monthly Baseline Service Volume by more than five percent (5%)).

2.2.5 Upset Limit

An upset range of +/- 20% of Monthly Baseline Service Volumes has been established. Actual Service Volumes above the upset range for three consecutive months, or below the upset range for three consecutive months, will trigger a re-establishment of the Monthly Baseline Service Volume, Variable Service Unit Cost and Variable Service Cost Adjustments (ARC and RRC) for the effected desk ("the Re-establishment"). For avoidance of doubt, triggering the upset limit will not impact the ARC or RRC otherwise calculated up to the last day of the third consecutive month triggering the Re-establishment. The Re-establishment of the (i) Monthly Baseline Service Volume, (ii) Variable Service Unit Cost, and (iii) Variable Service Cost Adjustments (ARC and RRC) shall be completed within 90 Calendars from the last day of the third consecutive month triggering the Re-establishment. The Contractor shall provide a proposal for the changes, and the Contractor and SSC shall act reasonably and in good faith to agree on the changes. The Contractor must provide support for the proposed changes and SSC shall have the right to audit such support. The agreed changes will apply retroactive to the first day of the first month following the third consecutive month triggering the Re-establishment.

Schedule B 2 – Service Level Requirements

Shared Services Canada (SSC)

Schedule B 2 – Service Level Requirements

Table of Contents

List of Examples

List of Tables

List of Formulas

Schedule B 2 – Service Level Requirements

1.0 Introduction

This Schedule describes the obligations of the Contractor with respect to Level of Service for the Service Desk Services described in **Schedule A 1 – Service Desk Services**.

2.0 Service Level Reporting

The Contractor will continuously monitor and measure its performance for all Service Categories. The format for reporting Level of Service is described in this Section.

2.1 Reporting Window

The Contractor will measure the Level of Service for each Service Category for each month of the Contract Term.

2.2 Report Format

The Contractor will provide reports, in soft-copy form, detailing the actual measured Level of Service for each Service Category for the prior month. Shared Services Canada (SSC) may request, at no additional cost to SSC, extracts of the underlying source data prepared in a sufficient manner to enable SSC to confirm the accuracy and completeness of the monthly Service Level Reports. Any changes to reporting required by SSC which results in the development or modification of reporting tools will be provided at no cost to SSC.

2.3 Report Deadline

Within five (5) Federal Government Working Days (FGWD) after the end of each month, the Contractor will provide a Service Level Report, in the prescribed manner.

2.4 Report Content

At a minimum, the Service Level Report must include the following:

(a) Calculation of the Level of Service, for the prior month, for all Service Categories.

(b) Identification of those Service Categories for which the Level of Service did not meet the Minimum Service Level ("Service Level Failure") in the prior month.

(c) Allocation of Percentages assigned by Shared Services Canada to each Service Category.

(d) Calculation of:

   a. Service Level Credit(s);

   b. Additional Service Level Credit(s); and

   c. Earn Back Amount(s).

(e) Details of any Excusable Event that the Contractor believes has impacted the Level of Service for any Service Category during the prior month.

(f) In addition to the prior month, the Contractor shall include 11 months of historical data for (a) through (c) above.

A sample monthly Service Level Report is provided in Section 13.

2.5 Notification of Failure (realized or imminent)

The Contractor must inform SSC immediately when it becomes aware that a Minimum Service Level has not been met, or will not be met in the current month.

3.0 Remediation Mechanism

The Contractor will be responsible for ensuring that performance meets or exceeds Minimum Service Levels in each month of the Contract Term. The mechanism for remediating Service Level Failures is described in this Section.

3.1 Responsibility for Remediation Activities

The Contractor is responsible for the cost and expense for all actions relating to the reporting and remediation of Service Level Failures.

3.2 Required Actions

In the instance of a Service Level Failure, the Contractor will:

(a) Perform a **Root Cause Analysis** to identify the cause of the Service Level Failure.

(b) Provide SSC with a written **Root Cause Analysis Report** detailing the cause of the Service Level Failure. The Root Cause Analysis Report will be provided to SSC (in a standardized format agreed to by SSC and the Contractor) within five (5) FGWDs from the date that SSC is notified that a Service Level Failure has occurred, or is imminent in a standardized format agreed to by SSC and the Contractor.

(c) Provide SSC with a **Corrective Action Plan** to prevent a recurrence of the Service Level Failure. The Corrective Action Plan will be provided to SSC (in a standardized format agreed to by SSC and the Contractor) within ten (10) FGWDs from the date that SSC is notified that a Service Level Failure has occurred, or is imminent.

(d) Implementation of the Corrective Action Plan within twenty (20) FGWDs of publication of the Corrective Action Plan. An implementation deadline greater than twenty (20) FGWDs may be permitted, subject to agreement by the Contractor and SSC.

(e) Provide SSC with weekly **Progress Reports** against the Corrective Action Plan (in a standardized format agreed to by SSC and the Contractor) in accordance with method and schedule to be agreed to by the Contractor and SSC.

3.3 Corrective Action Plan (Minimum Content)

At a minimum, the Corrective Action Plan must include the following:

(a) Planned Actions and related Milestone Deadlines.

(b) Details of proposed workarounds for an interim solution in advance of a permanent fix.

(c) Criteria for demonstrating ultimate resolution of the underlying problem that led to the Service Level Failure.

(d) Proposed method and schedule for issuance of periodic Progress Reports against the Corrective Action Plan.

3.4 Chronic Service Level Failures

In the event of Chronic Service Level Failures (2 or more consecutive months) for the same Service Level Category, the Contractor must deploy specialized management and non-operational resources to address chronic Service Level Failures. The Contractor will be responsible for the cost and expense of deploying these additional resources.

4.0 Service Level Credit Mechanism

This section outlines the Service Level Credit Mechanism.

4.1 Service Level Failure

Failure to meet or exceed the Minimum Service Level for any Service Level Category in any month will result in Service Level Credit owing from the Contractor to SSC.

4.2 Service Level Credit

The Service Level Credit shall be the product of the following:

Service Level Credit = Allocation Percentage for Service Category x At Risk Amount

4.3 Allocation Percentage

SSC shall allocate percentages to each Service Category to a sum total of 300%. SSC may allocate zero percent (0%) to a Service Level Category; however, the allocation to a given Service Category may not exceed one hundred percent (100%).

4.4 At Risk Amount

The At Risk Amount shall be fifteen percent (15%) of the total monthly charges for Service Desk Services for the month in which the Service Level Failure giving rise to the Service Level Credit occurred.

4.5 Monthly Limit

Multiple service level failures in a single month may result in multiple service level credits owing to SSC; however, in no instance shall the sum total of all Service Level Credits exceed fifteen percent (15%) of the total monthly charges for Service Desk Services for the month in which the multiple Service Level Failures giving rise the Service Level Credits occurred.

4.6 Sample Calculations for Service Level Credits

Sample Service Level Credit calculations for instances of (i) Single Service Level Failure, and (ii) Multiple Service Level Failures in a subject month follow:

Example 1: Service Level Credit(s) for Instance of Single Service Level Failure in Subject Month

In the month of January 20XX, the Contractor reports First Contract Resolution (FCR) Service Category performance at 79% for the Enterprise Service Desk. A Service Level Failure is reported as the Minimum Service Level for FCR is ≥ 85%.

Calculation of the applicable Service Level Credit is as follows:

January Invoice for ESD Services	$500,000	
At Risk Amount (15% of Invoice)	$75,000	A
Allocation Percentage for FCR Service Category	40%	B
Owing to SSC for FCR Service Level Failure [A x B]	$30,000	
TOTAL SERVICE LEVEL CREDIT OWING TO SCC FOR JANUARY 20XX	**$30,000**	

Example 2: Service Level Credit(s) for Instance of Single Service Level Failure in Subject Month

In the month of April 20XX, the Contractor reports Telephone Call Abandonment Rate Service Category performance at 8% and Customer Satisfaction Service Category performance at 75% for the End User Service Desk. Two Service Level Failures are reported as the Minimum Service Level for Telephone Call Abandonment Rate is ≤ 7.5% and the Minimum Service Level for Customer Satisfaction is ≥ 80%.

Calculation of the applicable Service Level Credit is as follows:

April 20XX Invoice for EUSD Services	$500,000	
At Risk Amount (15% of Invoice)	$150,000	A
Allocation Percentage for Telephone Call Abandon Rate Service Category	20%	B
Allocation Percentage for Customer Satisfaction Service Category	5%	C
Owing to SSC for Telephone Call Abandonment Rate Service Level Failure [A x B]	$30,000	
Owing to SSC for Customer Satisfaction Service Level Failure [A x C]	$7,500	
TOTAL SERVICE LEVEL CREDITS OWING TO SCC FOR APRIL 20XX	**$37,500**	

5.0 Consecutive Months

The section outlines the calculation of graduating Service Level Credits resulting from Service Level Failures for a given Service Level Category in consecutive months.

5.1 Service Level Failure in Second Consecutive Month

Failure to meet the Minimum Service Level for a given Service Level Category in two consecutive months will result in an Additional Service Level Credit in the second month equal to fifty percent (50%) of the Service Level Credit.

5.2 Service Level Failure in Third and Subsequent Consecutive Months

Failure to meet the Minimum Service Level for a given Service Level Category in three (3) or more consecutive months will result in an Additional Service Level Credit in the third and subsequent months equal to 100 percent (100%) of the Service Level Credit.

5.3 Termination for Service Level Failure

Where a Service Level Failure occurs for a given Service Level Category in any three (3) months in a rolling nine (9) month period, SSC shall be entitled to terminate this agreement upon notice to the Contractor.

5.4 Sample Calculations for Service Level Failures in Consecutive Months

Sample Service Level Credit calculations for instances of (i) Service Level Failure in Second Consecutive Month, and (ii) Service Level Failure in Third Consecutive Month follow:

Example 3: Service Level Failure in Second Consecutive Month

In the consecutive months of January 20XX and February 20XX, the Contractor reports First Contract Resolution (FCR) Service Category performance at 79% and 75% respectively, for the Enterprise Service Desk. Service Level Failures are reported in both months as the Minimum Service Level for FCR is ≥ 85%.

Calculation of the Additional Service Level Credit In February 20XX is as follows:

February 20XX Invoice for ESD Services	$650,000	
At Risk Amount (15% of Invoice)	$97,500	A
Allocation Percentage for FCR Service Category	40%	B
Credit Owing to SSC for FCR Service Level Failure [A x B]	$39,000	C
Additional Service Level Credit for 2nd Consecutive Month of Failure [C x 50%]	**$19,500**	
TOTAL SERVICE LEVEL CREDITS OWING TO SSC FOR FEBRUARY 20XX	$58,500	

Example 4: Service Level Failure in Third Consecutive Month

In the consecutive months of January 20XX, February 20XX and March 20XX, the Contractor reports First Contract Resolution (FCR) Service Category performance at 79%, 75% and 76% respectively, for the Enterprise Service Desk. Service Level Failures are reported in all three months as the Minimum Service Level for FCR is ≥ 85%.

Calculation of the Additional Service Level Credit In March 20XX is as follows:

March 20XX Invoice for EUSD Services	$625,000	
At Risk Amount (15% of Invoice)	$93,750	A
Allocation Percentage for FCR Service Category	40%	B
Credit Owing to SSC for FCR Service Level Failure [A x B]	$37,500	C
Additional Service Level Credit for 3rd Consecutive Month of Failure [C x 100%]	**$37,500**	
TOTAL SERVICE LEVEL CREDITS OWING TO SSC FOR MARCH 20XX	$75,000	

6.0 Service Level Earn Backs

The section outlines the Contractor's entitlement to the Earn Back of previously paid Service Level Credits.

6.1 Service Level Credit Earn Backs

Where the Contractor delivers service at or above the Minimum Service Level for a given Service Level Category in each of the three (3) months immediately following the month in which a Service Level Failure ("Originating Service Level Failure") has occurred for that given Service Level Category, the Contractor shall qualify for an Earn Back Amount.

6.2 Earn Back Amount

The Earn Back Amount shall be calculated at 100% of the sum of the Service Level Credit and Additional Service Level Credit (where applicable) arising from the Originating Service Level Failure.

6.3 Payment of Service Level Credits/Earn Back Amounts

Refer to Payment Terms and Conditions.

6.4 Sample Calculations for Earn Back of Service Level Credits

Sample Earn Back calculations for instances of (i) Single Service Failure, and (ii) Intervening Service Level Failure follow:

Example 5: Earn Back Amount for Single Service Level Failure for Subject Service Level Category

In the month of April 20XX, the Contractor reports a Service Level Failure for the Telephone Call Abandonment Rate Service Category for the Service Desk and a $30,000 Service Level Credit is issued by the Contractor to SSC. The Contractor then reports Telephone Abandonment Rate Service Category Performance at or in excess of the Minimum Service Level in each of the three subsequent months.

Calculation of the Earn Back Amount is as follows:

Service Level Credit Issued to SSC for Dispatch Rate for April 20XX	$30,000
Service Level Credit Issued to SSC for Dispatch Rate for May 20XX	nil
Service Level Credit Issued to SSC for Dispatch Rate for June 20XX	nil
Service Level Credit Issued to SSC for Dispatch Rate for July 20XX	nil
SERVICE LEVEL EARN BACK OWING TO CONTRACTOR IN JULY 20XX	**($30,000)**

Example 6: Earn Back Amount in the Instance of Intervening Service Level Failure

In the months of January and March 20XX, the Contractor reports Service Level Failures for the First Contact Resolution Service Category for the Service Desk. The Contractor issues Service Level Credits in the amounts of $30,000 and $35,000 respectively. The Contractor reports First Contact Resolution Service Category Performance at or in excess of the Minimum Service Level in February 20XX and for April through June of 20XX.

Calculation of the Earn Back Amount is as follows:

Service Level Credit Issued to SSC for Reopened Tickets for January 20XX*Note 1*	$30,000
Service Level Credit Issued to SSC for Reopened Tickets for February 20XX	nil
Service Level Credit Issued to SSC for Reopened Tickets for March 20XX	$35,000
Service Level Credit Issued to SSC for Reopened Tickets for April 20XX	nil
Service Level Credit Issued to SSC for Reopened Tickets for May 20XX	nil
Service Level Credit Issued to SSC for Reopened Tickets for June 20XX	nil
SERVICE LEVEL EARN BACK OWING TO CONTRACTOR IN JUNE 20XX	**($35,000)**

Note 1: The intervening failure during the three months subsequent to January 20XX disqualifies the Service Provider from recovering the January 20XX Service Level Credit.

7.0 Excusable Event

This section outlines the treatment of Excusable Events in the calculation of Service Level Credits.

7.1 Definition of Excusable Event

An “Excusable Event” means those events or circumstances outside the reasonable control of the Contractor, including a Force Majeure Event (excepting a strike or other labour disturbance directly or indirectly relating to the Contractor’s business), to the extent excused in accordance with the Contract. For greater clarity, a labour action shall not constitute an excusable event.

If the Contractor’s Level of Service for a Service Level Category(s) shall be affected by a condition of Force Majeure, the Contractor shall give SSC immediate notification thereof, which notification shall contain the Contractor estimate of the duration of such condition and a description of the steps being taken or proposed to be taken to overcome such condition of Force Majeure. A condition of Force Majeure shall be deemed to continue only so long as the Contractor is taking reasonable actions necessary to overcome such condition.

Any reasonable impact to the Level of Service occasioned by any such cause shall not constitute a Service Level Failure, and the Minimum Service Level(s) for the affected Service Level Category(s) shall be suspended during the period of impact so occasioned.

If the Contractor’s Level of Service is impacted by Force Majeure, the realized Level of Service shall be discussed at the next monthly Service Desk Service Operations Committee meeting to agree on the exemption of the impacted Service Level Category(s) during the period of impact and record the decision.

7.2 Service Failure Outside the Control of the Contractor

Where the performance of the Contractor is impacted by an Excusable Event(s) in any given month, SSC may, at its discretion, agree to:

(a) Forfeit of entitlement to any Service Level Credit(s) otherwise owing for the impacted month(s); or

(b) Adjustment(s) to the calculation of Level of Service for the impacted Service Level Category(s) for that portion of the month(s) not impacted by the Excusable Event.

8.0 Service Level Requirements for the Enterprise Service Desk

This section details the Service Level Requirements for the Enterprise Service Desk:

Table 88: ESD Service Level Requirements

ESD SERVICE CATEGORY		MINIMUM SERVICE LEVEL		MEASUREMENT WINDOW	ALLOCATION PERCENTAGE
		PERFORMANCE TARGET	PERCENTAGE ACHIEVED		
First Contact Resolution		*Resolvable Tickets*	*≥ 85%*	*Monthly*	*30%*
Re-opened Tickets		*3 business days*	*≤ 5%*	*Monthly*	*20%*
Telephone Call Answer Rate	*Base*	*45 seconds or less*	*≥ 85%*	*Monthly*	*30%*
	Ceiling	*120 Seconds or less*	*≥ 98%*	*Monthly*	*20%*
Chat Answer Rate	*Base*	*45 seconds or less*	*≥ 85%*	*Monthly*	*0%*
	Ceiling	*120 seconds or less*	*≥ 98%*	*Monthly*	*0%*
Email Response Rate	*Base*	*1 hour or less*	*≥ 90%*	*Monthly*	*30%*
	Ceiling	*4 hours or less*	*≥ 98%*	*Monthly*	*20%*
Self-Service Portal Response Rate	*Base*	*1 hour or less*	*≥ 90%*	*Monthly*	*30%*
	Ceiling	*4 hours or less*	*≥ 98%*	*Monthly*	*20%*
Telephone Call Abandonment Rate		*Greater than 60 seconds*	*≤ 5%*	*Monthly*	*30%*
Chat Abandonment Rate		*Greater than 60 seconds*	*≤ 5%*	*Monthly*	*0%*
Customer Satisfaction		*CSAT Score*	*≥ 85%*	*Monthly*	*40%*
Quality Assurance		*QA Score*	*≥ 80%*	*Monthly*	*30%*
TOTAL PERCENTAGE ALLOCATION FOR ALL ESD SERVICE CATEGORIES					**300%**

9.0 Service Level Requirements for the End User Service Desk

This section details the Service Level Requirements for the End User Service Desk:

Table 89: EUSD Service Level Requirements

EUSD SERVICE CATEGORY		MINIMUM SERVICE LEVEL		MEASUREMENT WINDOW	ALLOCATION PERCENTAGE
		PERFORMANCE TARGET	PERCENTAGE ACHIEVED		
First Contact Resolution		*Resolvable Tickets*	*≥ 85%*	*Monthly*	*30%*
Re-opened Tickets		*3 business days*	*≤ 5%*	*20%*	*20%*
Telephone Call Answer Rate	*Base*	*45 seconds or less*	*≥ 85%*	*30%*	*30%*
	Ceiling	*120 Seconds or less*	*≥ 98%*	*20%*	*20%*
Chat Answer Rate	*Base*	*45 seconds or less*	*≥ 85%*	*0%*	*0%*
	Ceiling	*120 seconds or less*	*≥ 98%*	*0%*	*0%*
Email Response Rate	*Base*	*1 hour or less*	*≥ 90%*	*30%*	*30%*
	Ceiling	*4 hours or less*	*≥ 98%*	*20%*	*20%*
Self-Service Portal Response Rate	*Base*	*1 hour or less*	*≥ 90%*	*30%*	*30%*
	Ceiling	*4 hours or less*	*≥ 98%*	*20%*	*20%*
Telephone Call Abandonment Rate		*Greater than 60 seconds*	*≤ 5%*	*Monthly*	*30%*
Chat Abandonment Rate		*Greater than 60 seconds*	*≤ 5%*	*Monthly*	*0%*
Customer Satisfaction		*CSAT Score*	*≥ 85%*	*Monthly*	*40%*
Quality Assurance		*QA Score*	*≥ 80%*	*Monthly*	*30%*
TOTAL PERCENTAGE ALLOCATION FOR ALL EUSD SERVICE CATEGORIES					**300%**

10.0 Formulas for Calculating Service Level Performance

This section describes the formulas for calculating Service Level Performance:

Formula 1: First Contact Resolution

The intent of this metric is to ensure all Service Desk personnel have the skills, training and knowledge necessary to resolve tickets upon first contact without escalation or dispatch			
FORMULA	$\frac{\textit{Total Number of Resolvable Tickets Resolved on First Contact} - \textit{Callbacks Within 24 Hours}}{\textit{Total Number of Resolvable Tickets Answered}}$ x 100%		
Data Element 1:	Total Number of Resolvable Tickets Resolved on First Contact	Data Source:	ITSM Tool
Data Element 2:	Call-backs Within 24 Hours	Data Source:	ITSM Tool
Data Element 3:	Total Number of Resolvable Tickets Answered	Data Source:	ITSM Tool
Notes:	See SCHEDULE A 13 – TYPES OF CONTACTS HANDLED for resolvable and non-resolvable ticket types.		

Formula 2: Re-opened Tickets

The intent of this metric is to ensure that tickets that the Service Desk has resolved are not marked as “resolved” before they are effectively resolved and resolution has been validated by the end user.

FORMULA	$\frac{\textit{Total Number of Tickets Re-opened by the Service Desk}}{\textit{Total Number of Tickets Resolved by the Service Desk}}$ x 100%		
Data Element 1:	Total Number of Tickets Re-opened by the Service Desk	Data Source:	ITSM Tool
Data Element 2:	Total Number of Tickets Resolved by the Service Desk	Data Source:	ITSM Tool

Formula 3: Telephone Call Answer Rate

The intent of this metric is to ensure that service desk agents can be reached quickly by telephone.			
FORMULA	$\frac{\textit{Total Number of Calls Answered by Service Desk Personnel Within Performance Target of Entering the Queue}}{\textit{Total Number of Calls Answered by Service Desk Personnel}}$ x 100%		
Data Element 1:	Total Number of Calls Answered by Service Desk Personnel Within Performance Target of Entering the Queue	Data Source:	Telephony Platform
Data Element 2:	Total Number of Calls Answered by Service Desk Personnel	Data Source:	Telephony Platform

Formula 4: Chat Answer Rate

The intent of this metric is to ensure that service desk agents can be reached quickly by chat.			
FORMULA	$\frac{\textit{Total Number of Chats Responded by Service Desk Personnel Within Performance Target of Entering the Queue}}{\textit{Total Number of Chats Responded by Service Desk Personnel}}$ x 100%		
Data Element 1:	Total Number of Chats responded by Service Desk Personnel Within Performance Target of Entering the Queue	Data Source:	ITSM Tool
Data Element 2:	Total Number of Chats Responded by Service Desk Personnel	Data Source:	ITSM Tool

Formula 5: Email Response Rate

The intent of this metric is to ensure the timely response to requests sent to the Service Desk via Email.			
FORMULA	$\frac{\textit{Total Number of Emails Responded by Service Desk Personnel Within Performance Target of Entering the Queue}}{\textit{Total Number of Emails Responded by Service Desk Personnel}}$ x 100%		
Data Element 1:	Total Number of Emails responded by Service Desk Personnel Within Performance Target of Entering the Queue	Data Source:	ITSM Tool
Data Element 2:	Total Number of Emails Responded by Service Desk Personnel	Data Source:	ITSM Tool

Formula 6: Self-Service Portal Response Rate

The intent of this metric is to ensure the timely response to requests sent to the Service Desk via self-service portal.			
FORMULA	$\frac{\textit{Total Number of Tickets Created Via Self-Service Portal Where Response Occurred Within Performance Target}}{\textit{Total Number of Tickets Created Via Self-Service Portal}}$ x 100%		
Data Element 1:	Total Number of Tickets Created Via Self-Service Portal Where Response Occurred Within Performance Target	Data Source:	ITSM Tool
Data Element 2:	Total Number of Tickets Created Via Self-Service Portal	Data Source:	ITSM Tool

Formula 7: Telephone Call Abandonment Rate

The intent of this metric is to monitor and reduce the number of abandoned calls and to ensure calls are answered by Service Desk personnel within the Performance Target.			
FORMULA	$\frac{\textit{Total Number of Calls Abandoned After Performance Target of Entering the Queue}}{\textit{Total Number of Calls Queued More than Performance Target of Entering the Queue}}$ x 100%		
Data Element 1:	Total Number of Calls Abandoned After Performance Target of Entering the Queue	Data Source:	Telephony Platform
Data Element 2:	Total Number of Calls Queued More than Performance Target of Entering the Queue	Data Source:	Telephony Platform

Formula 8: Chat Abandonment Rate

The intent of this metric is to monitor and reduce the number of abandoned chats and to ensure chats are answered by Service Desk personnel within the Performance Target.			
FORMULA	$\frac{\textit{Total Number of Chats Abandoned After 60 Seconds of Entering the Queue}}{\textit{Total Number of Chats Queued More than 60 Seconds of Entering the Queue}}$ x 100%		
Data Element 1:	Total Number of Chats Abandoned After Performance Target of Entering the Queue	Data Source:	ITSM Tool
Data Element 2:	Total Number of Chats Queued More than Performance Target of Entering the Queue	Data Source:	ITSM Tool

Formula 9: Customer Satisfaction

The intent of this metric is to ensure that customers are receiving service that meets their expectations.			
FORMULA	$\frac{\textit{Sum of Customer Satisfaction Survey Scores (CSAT) for all Completed Surveys}}{\textit{Total Number of Completed CSAT Surveys}}$ x 100%		
Data Element 1:	Sum of Customer Satisfaction Survey Scores (CSAT) for all Completed Surveys	Data Source:	CSAT Repository
Data Element 2:	Total Number of Completed CSAT Surveys	Data Source:	CSAT Repository
Notes:	See SCHEDULE A 3 – TRANSITION SERVICES Section 3.1.4 Service Transition Approach per Statement of Work.		

Formula 10: Quality Assurance

The intent of this metric is to ensure that customers are receiving high quality service.			
FORMULA	$\frac{\textit{Sum of Qualifty Assurance (QA) Scores Conducted}}{\textit{Total Number of QA Scorings Conducted}}$ x 100%		
Data Element 1:	Sum of Quality Assurance (QA) Scores Conducted	Data Source:	QA Repository
Data Element 2:	Total Number of QA Scorings Conducted	Data Source:	QA Repository
Notes:	See SCHEDULE A 3 – TRANSITION SERVICES Section 3.1.4 Service Transition Approach per Statement of Work.		

11.0 Continuous Service Improvement

The Minimum Service Level for the First Contact Resolution (FCR), Customer Satisfaction (CSAT) and Quality Assurance (QA) Service Level Categories will automatically increase on the anniversary date of the contract. The increase will be calculated at 10% of the difference between perfection (100%) and the then current Minimum Service Level for the respective Service Level Category.

12.0 Change Process

This section describes the process for changing Service Level Requirements.

12.1 Semi-Annual Review of Service Level Requirements

Shared Services Canada (SSC) and the Contractor will meet twice a year to review Service Level Requirements and make allowable changes at that time. SSC and the Contractor shall agree on the dates for semi-annual reviews.

12.2 Changes to Service Level Requirements

Shared Services Canada (SSC) may add, delete or modify Service Level Requirements as follows:

(a) Add a new Service Level Category or delete any existing Service Level Category;

(b) Modify the Allocation Percentage for any Service Level Category;

(c) Make a change to the Minimum Service Level for any Service Level Category.

12.3 Add a new Service Level Category or delete any existing Service Level Category

The addition or substitution of new Service Level Categories by Shared Services Canada in accordance with this Section shall be in order to achieve a fair, accurate and consistent measurement of the Contractor's performance for the services. For example, such additions or substitutions may occur in conjunction with changes to the environment and the introduction of new tools, technology or channels of service delivery; provided, however, that where such new tools, technology or channels of service delivery are a replacement or upgrade of existing technology, there shall be a presumption of equivalent or improved performance.

12.4 Modify the Allocation Percentage for any Service Level Category

The modification of Allocation Percentages for Service Level Categories shall allow SSC to signal changes in priorities over time. Modification of Allocation of Percentages for Service Level Categories shall not be subject to Change Control Procedures.

12.5 Make a Change to the Minimum Service Level for any Service Level Category

The modification of Minimum Service Level for Service Level Categories shall allow SSC to signal changes in performance expectations over the term of the Contract.

12.6 Change Control Procedures

Any change made pursuant to this section will be subject to the Change Control Procedures (with the exception of modifications to allocation percentages between Service Level Categories). For clarity, the modification of Allocation Percentages between Service Level Categories will not be a Change subject to the Change Control Procedures.

13.0 Sample Monthly Service Level Report

The following sample Service Level Report is provided for illustration purposes only:

Example 7: Sample Monthly Service Level Report

SERVICE CATEGORY		MINIMUM SERVICE LEVEL		JAN XX	FEB XX	MAR XX	APR XX	MAY XX	JUN XX	JUL XX	AUG XX	SEP XX	OCT XX	NOV XX	DEC XX
		PERFORMANCE TARGET	PERCENTAGE ACHIEVED												
First Contact Resolution		Resolvable Tickets	≥ 85%	79.0	75.0	76.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0
Re-opened Tickets		Resolved Tickets	≤ 5%	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
Telephone Call Answer Rate	Base	≤ 45 seconds	≥ 85%	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0
	Ceiling	≤ 120 seconds	≥ 98%	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0
Chat Answer Rate	Base	≤ 45 seconds	≥ 85%	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0
	Ceiling	≤ 120 seconds	≥ 98%	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0
Email Response Rate	Base	≤ 1 hour	≥ 90%	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0
	Ceiling	≤ 4 hours	≥ 98%	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0
Self-Service Portal Response Rate	Base	≤ 1 hour	≥ 90%	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0	90.0
	Ceiling	≤ 4 hours	≥ 98%	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0	98.0
Telephone Call Abandonment Rate		> 60 seconds	≤ 5%	5.0%	5.0	5.0	8.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
Chat Abandonment Rate		> 60 seconds	≤ 5%	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
Customer Satisfaction		CSAT Score	≥ 85%	85.0	85.0	85.0	75.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0
Quality Assurance		QA Score	≥ 80%	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0	80.0

				SERVICE LEVEL CREDIT / EARN BACK AS A PERCENTAGE OF INVOICE											
SERVICE CATEGORY		CREDIT AMOUNT		JAN XX	FEB XX	MAR XX	APR XX	MAY XX	JUN XX	JUL XX	AUG XX	SEP XX	OCT XX	NOV XX	DEC XX
		ALLOCATION PERCENTAGE	AT RISK AMOUNT												
First Contact Resolution		40%	15% of Invoice	6%	9%	12%	-	-	12%	-	-	-	-	-	-
Re-opened Tickets		20%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
Telephone Call Answer Rate	Base	30%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
	Ceiling	15%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
Chat Answer Rate	Base	30%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
	Ceiling	15%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
Email Response Rate	Base	30%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
	Ceiling	15%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
Self-Service Portal Response Rate	Base	30%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
	Ceiling	15%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
Telephone Call Abandonment Rate		20%	15% of Invoice	-	-	-	3%	-	-	3%	-	-	-	-	-
Chat Abandonment Rate		20%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
Customer Satisfaction		20%	15% of Invoice	-	-	-	3%	-	-	3%	-	-	-	-	-
Quality Assurance		0%	15% of Invoice	-	-	-	-	-	-	-	-	-	-	-	-
TOTAL ALLOCATION		300%													

14.0 Consistency of Service

14.1 Language

The Enterprise and End User Service Desks must provide support services to users in the official language of their choice. Those support services must be of equal quality and level of service, regardless of the language chosen.

14.2 End User Service Desk

The End User Service Desk must provide support services to users of the following Partners:

- Public Service and Procurement Canada;
- Health Canada;
- Shared Services Canada;
- Canada School of Public Service; and
- Infrastructure Canada.

Those support services must be of equal quality and level of service, regardless of the department from which the user resides.

Schedule B 3 – Financial Responsibility Matrix

Shared Services Canada (SSC)

Schedule B 3 – Financial Responsibility Matrix

Table of Contents

List of Tables

Schedule B 3 – Financial Responsibility Matrix

This Schedule describes the financial responsibilities of the Contractor and Shared Services Canada (SSC) with respect to hardware and software utilized by the Enterprise Service Desk (ESD) and the End User Service Desk (EUSD) to provide Service Desk Services described in **Schedule A 1 – Service Desk Services**.

1.0 ESD Financial Responsibility Matrix

The Service Desk Services described in **Schedule A1 – Service Desk Services** include participation from both SSC and the Contractor. The following table establishes responsibility for the acquisition, operation and maintenance of hardware and software required to deliver the Service Desk Services. The following table contains the current list of tools used and this list may change over time.

Responsibilities are separated into the following categories:

- Asset Ownership – party responsible for acquisition of the indicated Hardware / Software;
- Upgrades/Enhancements – party responsible ensuring that the indicated Hardware / Software is current (N-1 version, security patches applied etc.);
- Technology Refreshment – party is responsible for ensuring that technology is up-to-date and compatible with new issuances; and
- Charging Mechanism – indicates whether cost is born by the Contractor and recovered as part of the monthly fees charged to SSC (see **Schedule B 1 – Pricing Provisions**).

Table 90: ESD Hardware and Software/Applications

Type of Asset	Asset Ownership	Financial Responsibility		
		Upgrades / Enhancements	Technology Refreshment	Charging Mechanism
Service Desk Portal Hardware: Citrix Server	SSC	SSC	SSC	N/A
Workstation (Contractor Service Location)	Contractor	Contractor	Contractor	Included in Cost per Contact
Microsoft Windows Operating System (currently version 10)	Contractor	Contractor	Contractor	Included in Cost per Contact
Internet Explorer (and necessary plug-ins)	Contractor	Contractor	Contractor	Included in Cost per Contact
Google Chrome Explorer (and necessary plug-ins)	Contractor	Contractor	Contractor	Included in Cost per Contact
Mozilla Firefox Explorer (and necessary plug-ins)	Contractor	Contractor	Contractor	Included in Cost per Contact
Citrix Receiver / Citrix Workspace	Contractor	Contractor	Contractor	Included in Cost per Contact
Third Party Second Factor Authenticator Application	Contractor	Contractor	Contractor	Included in Cost per Contact
Contractor Management Tools	Contractor	Contractor	Contractor	Included in Cost per Contact
Service Desk Portal Software and Operating Systems	SSC	SSC	SSC	N/A

Microsoft Office Professional (Outlook, Word, Excel, Access)	SSC	SSC	SSC	N/A
Video-conferencing Software: WebEx	SSC	SSC	SSC	N/A
Collaboration Software: Jabber	SSC	SSC	SSC	N/A
ITSM Tool for On-Boarded Partners: IBM Tivoli Enterprise Control Desk (ECD)	SSC	SSC	SSC	N/A
ITSM Tool for Legacy (GOP) Partners: InfoWeb	SSC	SSC	SSC	N/A
Knowledge Database: Get Answers	SSC	SSC	SSC	N/A
Knowledge Database: GC Docs	SSC	SSC	SSC	N/A
Incident Management Priority Matrix	SSC	SSC	SSC	N/A
Critical Business Applications and Services (CBAS) List	SSC	SSC	SSC	N/A
Designated Sites (DS) List	SSC	SSC	SSC	N/A
Data Centre Site (DC) List	SSC	SSC	SSC	N/A
Real Time Contact List (RTCL)	SSC	SSC	SSC	N/A
Single Point of Contact / Partner Major Incident Coordinator (SPOC/PMIC) List	SSC	SSC	SSC	N/A
ECD Resolver Group List	SSC	SSC	SSC	N/A
Change Management List	SSC	SSC	SSC	N/A
Operational Data Store (Operational CMDB)	SSC	SSC	SSC	N/A
SSC Home Page	SSC	SSC	SSC	N/A
Network Equipment				
GC WAN Hardware	SSC	SSC	SSC	N/A
Internet Connectivity (Contractor to SSC)	Contractor	Contractor	Contractor	Included in Cost per Contact
Security Equipment				
Security Hardware (SSC Locations)	SSC	SSC	SSC	N/A
Security Hardware (Contractor Service Locations)	Contractor	Contractor	Contractor	Included in Cost per Contact
Security Software				
Entrust on Contractor Desktop Devices	SSC	SSC	SSC	N/A
Anti-virus (Contractor Service Locations)	Contractor	Contractor	Contractor	Included in Cost per Contact
Voice Equipment				
Contact Centre Telephony Solution	SSC	SSC	SSC	N/A
Toll-Free Number	SSC	SSC	SSC	N/A

Telephones/Headsets (Contractor Service Location)	Contractor	Contractor	Contractor	Included in Cost per Contact
Contractor Site Telephony Infrastructure (e.g. PBX)	Contractor	Contractor	Contractor	Included in Cost per Contact

2.0 EUSD Financial Responsibility Matrix

The Service Desk Services described in **Schedule A1 – Service Desk Services** includes participation from both SSC and the Contractor. The following table establishes responsibility for the acquisition, operation and maintenance of hardware and software required to deliver the Service Desk Services. The following table contains the current list of tools used and this list may change over time.

Responsibilities are separated into the following categories:

- Asset Ownership – party responsible for acquisition of the indicated Hardware / Software;
- Upgrades/Enhancements – party responsible ensuring that the indicated Hardware / Software is current (N-1 version, security patches applied etc.);
- Technology Refreshment – party is responsible for ensuring that technology is up-to-date and compatible with new issuances; and
- Charging Mechanism – indicates whether cost is born by the Contractor and recovered as part of the price charged to SSC (see **Schedule B 1 – Pricing Provisions**).

Table 91: EUSD Hardware and Software/Applications

Type of Asset	Asset Ownership	Financial Responsibility		
		Upgrades / Enhancements	Technology Refreshment	Charging Mechanism
Service Desk Portal Hardware: Citrix Server	SSC	SSC	SSC	N/A
Workstation (Contractor Service Location)	Contractor	Contractor	Contractor	Included in Cost per Contact
Microsoft Windows Operating System (currently version 10)	Contractor	Contractor	Contractor	Included in Cost per Contact
Internet Explorer (and necessary plug-ins)	Contractor	Contractor	Contractor	Included in Cost per Contact
Google Chrome(and necessary plug-ins)	Contractor	Contractor	Contractor	Included in Cost per Contact
Mozilla Firefox(and necessary plug-ins)	Contractor	Contractor	Contractor	Included in Cost per Contact
Citrix Receiver / Citrix Workspace	Contractor	Contractor	Contractor	Included in Cost per Contact
Third Party Second Factor Authenticator Application	Contractor	Contractor	Contractor	Included in Cost per Contact
Contractor Management Tools	Contractor	Contractor	Contractor	Included in Cost per Contact
Service Desk Portal Software and Operating Systems	SSC	SSC	SSC	N/A
Microsoft Office Professional (Outlook, Word, Excel, Access)	SSC	SSC	SSC	N/A

Video-conferencing Software: WebEx	SSC	SSC	SSC	N/A
Collaboration Software: Jabber	SSC	SSC	SSC	N/A
ITSM Tool: Micro Focus Service Manager	SSC	SSC	SSC	N/A
Remote Takeover Tool: System Centre Configuration Manager (SCCM) 2012 R2 Remote Control	SSC	SSC	SSC	N/A
Account Administration: Canada.ca Admin Portal	SSC	SSC	SSC	N/A
Account Administration: Active Directory Users and Computers	SSC	SSC	SSC	N/A
Account Administration: iManager	SSC	SSC	SSC	N/A
Account Administration: Sigma	SSC	SSC	SSC	N/A
Service Catalogue: Government of Canada Express (GCSX)	SSC	SSC	SSC	N/A
Service Catalogue: Office Systems Service Request Online (OSSRO)	SSC	SSC	SSC	N/A
Knowledge Database: Confluence	SSC	SSC	SSC	N/A
Service Desk Portal Software and Operating Systems	SSC	SSC	SSC	N/A
Microsoft Office Professional (Outlook, Word, Excel, Access)	SSC	SSC	SSC	N/A
Video-conferencing Software: WebEx	SSC	SSC	SSC	N/A
Collaboration Software: Jabber	SSC	SSC	SSC	N/A
IBM Big Fix Remote [Remote Takeover Tool]	SSC	SSC	SSC	N/A
IBM Web Reports [TEM]	SSC	SSC	SSC	N/A
SDP Bell Portal [Email Password / EMDM Password]	SSC	SSC	SSC	N/A
iManager [Novell Password Resets]	SSC	SSC	SSC	N/A
Bitlocker [Password Reset]	SSC	SSC	SSC	N/A
ITSM Ticketing Tool: HP Openview Service Centre (SM6)	SSC	SSC	SSC	N/A
Iprint [Network Printer Installations]	SSC	SSC	SSC	N/A
Hyper Snap [Screen Shot Capture]	SSC	SSC	SSC	N/A
Notepad [Create Templates and Paste in Tickets]	SSC	SSC	SSC	N/A
ShortKeys [Apply Templates for Calls]	SSC	SSC	SSC	N/A
Cisco AnyConnect [VPN Access]	SSC	SSC	SSC	N/A
Lotus Notes [Various]	SSC	SSC	SSC	N/A
GC WAN Hardware	SSC	SSC	SSC	N/A
Internet Connectivity (Contractor to SSC)	Contractor	Contractor	Contractor	Included in Cost per Contact

Security Equipment				
Security Hardware (SSC Locations)	SSC	SSC	SSC	N/A
Security Hardware (Contractor Service Locations)	Contractor	Contractor	Contractor	Included in Cost per Contact
Security Software				
Entrust on Contractor Desktop Devices	SSC	SSC	SSC	N/A
Anti-virus (Contractor Service Locations)	Contractor	Contractor	Contractor	Included in Cost per Contact
Voice Equipment				
Contact Centre Telephony Solution	SSC	SSC	SSC	N/A
Toll-Free Number(s)	SSC	SSC	SSC	N/A
Telephones/Headsets (Contractor Service Location)	Contractor	Contractor	Contractor	Included in Cost per Contact
Contractor Site Telephony Infrastructure (e.g. PBX)	Contractor	Contractor	Contractor	Included in Cost per Contact

Schedule B 4 – Reporting

Shared Services Canada (SSC)

Schedule B 4 – Reporting

Table of Contents

List of Tables

Schedule B 4 – Reporting

This Schedule describes reporting responsibilities associated with the Service Desk Services described in **Schedule A 1 – Service Desk Services**.

1.0 Metrics Repository

The Contractor shall be responsible for obtaining analytics from the following systems of record: ITSM Tools, Telephony Reporting Platforms and Service Catalogues, for the purposes of completing monthly Service Level Requirements (SLR) and Key Performance Indicator (KPI) reporting.

Analytic data obtained by the Contractor for the purposes of completing monthly Service Level Requirements (SLR) and periodic Key Performance Indicator (KPI) reporting shall be retained by the Contractor in a metrics repository provisioned by SSC for that purpose.

The metrics repository shall be organized into a searchable database in chronological order from contract inception through to the end of the Contract Term. The Contractor shall partition the metrics repository into ESD and EUSD segments with the EUSD segment further partitioned into five End User Customer segments: Public Service and Procurement Canada (PSPC), Health Canada (HC), Shared Services Canada (SSC), Canada School of Public Service (CSPS) and Infrastructure Canada (INFC). Any changes to reporting required by SSC which results in the development or modification of reporting tools will be provided at no cost to SSC.

The Contractor shall ensure that updates to the metrics repository are aligned with SLR and KPI reporting timelines. In other words, SSC must be able to reconcile SLR and KPI report content to the source information in the metrics repository immediately upon issuance of those reports.

2.0 Monthly SLR Reporting

The Contractor will continuously monitor and measure its performance for all Service Categories. The format for reporting Level of Service is described in **Schedule B 2 – Service Level Requirements** and re-produced here:

2.1 SLR Reporting Window

The Contractor will measure the Level of Service for each Service Category for each month of the Contract Term.

2.2 SLR Report Format

The Contractor will provide reports, in soft-copy form, detailing the actual measured Level of Service for each Service Category for the prior month. Shared Services Canada (SSC) may request, at no additional cost to SSC, extracts of the underlying source data prepared in a sufficient manner to enable SSC to confirm the accuracy and completeness of the monthly Service Level Reports. Any changes to reporting required by SSC which results in the development or modification of reporting tools will be provided at no cost to SSC.

2.3 SLR Reporting Deadline

Within five (5) Federal Government Working Days (FGWD) after the end of each month, the Contractor will provide a Service Level Report, in the prescribed manner.

2.4 SLR Report Content

At a minimum, the Service Level Report must include the following:

(a) Calculation of the Level of Service, for the prior month, for all Service Categories.

(b) Identification of those Service Categories for which the Level of Service did not meet the Minimum Service Level ("Service Level Failure") in the prior month.

(c) Allocation Percentages assigned by Shared Services Canada to each Service Category.

(d) Calculation of:

I. Service Level Credit(s);

II. Additional Service Level Credit(s); and

III. Earn Back Amount(s).

(e) Details of any Excusable Event that the Contractor believes has impacted the Level of Service for any Service Category during the prior month.

(f) In addition to the prior month, the Contractor shall include 11 months of historical data for (a) through (c) above.

A sample Monthly Service Level Report is provided in Section 11 of **Schedule B 2 – Service Level Requirements**.

3.0 Periodic KPI Reporting

The Contractor will continuously monitor and measure its performance for all Key Performance Indicators. Consistent performance issues on relating to KPIs will be addressed through the SSC Governance and Relationship Management Services (**See Schedule A 4 – Governance and Relationship Management Services).** SSC and the Contractor will review the KPIs performance every six months or in greater frequency as agreed between SSC and the Contractor. Any remediation and action items generated to address the KPI performance issues and approved by SSC will be implemented by the Contractor as part of the service improvement objective at no extra cost for SSC.

3.1 ESD KPI Report Content

The Contractor shall prepare, in soft copy form, KPI Reports containing the following analytic data for the intervals indicated:

Table 92: ESD KPI Reporting

	Key Performance Indicator	Category	Daily	Weekly	Monthly
1.0	**Number of Abandoned Calls**	Workload	✓	✓	✓
1.1	Calls Abandoned in 60 seconds or less	Workload	✓	✓	✓
1.2	Calls Abandoned in greater than 60 seconds	Workload	✓	✓	✓
1.3	Average Time to Abandon Call	Performance Indicator	✓	✓	✓
1.4	Call Abandonment Rate	Performance Indicator	✓	✓	✓
2.0	**Number of Calls Answered by Service Desk Agents**	Workload	✓	✓	✓
2.1	Average Wait Time	Performance Indicator	✓	✓	✓
2.2	Average Talk Time	Performance Indicator	✓	✓	✓
2.3	Average Handle Time (including wrap-up)	Performance Indicator	✓	✓	✓
2.4	Percentage of Calls Answered in Base Target: 45 seconds or less	Performance Indicator	✓	✓	✓
2.5	Percentage of Calls Answered in Ceiling Target: 120 seconds or less	Performance Indicator	✓	✓	✓

	Key Performance Indicator	Category	Daily	Weekly	Monthly
2.6	Month-to-Date Percentage of Calls Answered in Base Target: 45 seconds or less	Performance Indicator	✓	-	-
2.7	Month-to-Date Percentage of Calls Answered in Ceiling Target: 120 seconds or less	Performance Indicator	✓	-	-
3.0	**Number of Abandoned Chats**	Workload	✓	✓	✓
3.1	Chats Abandoned in 60 seconds or less	Workload	✓	✓	✓
3.2	Chats Abandoned in greater than 60 seconds	Workload	✓	✓	✓
3.3	Average Time to Abandon Chat	Performance Indicator	✓	✓	✓
3.4	Chat Abandonment Rate	Performance Indicator	✓	✓	✓
4.0	**Number of Chats Answered by Service Desk Agents**	Workload	✓	✓	✓
4.1	Average Wait Time	Performance Indicator	✓	✓	✓
4.2	Average Chat Time	Performance Indicator	✓	✓	✓
4.3	Average Handle Time (including wrap-up)	Performance Indicator	✓	✓	✓
4.4	Percentage of Chats Answered in Base Target: 45 seconds or less	Performance Indicator	✓	✓	✓
4.5	Percentage of Chats Answered in Ceiling Target: 120 seconds or less	Performance Indicator	✓	✓	✓
4.6	Month-to-Date Percentage of Chats Answered in Base Target: 45 seconds or less	Performance Indicator	✓	-	-
4.7	Month-to-Date Percentage of Chats Answered in Ceiling Target: 120 seconds or less	Performance Indicator	✓	-	-
5.0	**Number of Emails Deemed Not Actionable**	Channel Efficacy	✓	✓	✓
6.0	**Number of Emails Responded by Service Desk Agents (without automation)**	Workload	✓	✓	✓
6.1	Percentage of Emails Responded within Base Target: 1 hour or less	Performance Indicator	✓	✓	✓
6.2	Percentage of Emails Responded within Ceiling Target: 4 hours or less	Performance Indicator	✓	✓	✓
6.3	Month-to-Date Percentage of Emails Responded within Base Target: 1 hour or less	Performance Indicator	✓	-	-
6.4	Month-to-Date Percentage of Emails Responded to within Ceiling Target: 4 hours or less	Performance Indicator	✓	-	-
7.0	**Number of Self-Service Portal Requests Responded by Service Desk Agents**	Workload	✓	✓	✓
7.1	Percentage of Self-Service Portal Requests Responded within Base Target: 1 hour or less	Performance Indicator	✓	✓	✓
7.2	Percentage of Self-Service Portal Responded within Ceiling Target: 4 hours or less	Performance Indicator	✓	✓	✓
7.3	Month-to-Date Percentage of Self-Service Portal Requests Responded within Base Target: 1 hour or less	Performance Indicator	✓	-	-
7.4	Month-to-Date Percentage of Self-Service Portal Requests Responded within Ceiling Target: 4 hours or less	Performance Indicator	✓	-	-
8.0	**Total Number of Contacts[Note] [2.0 + 4.0 + 6.0 + 7.0]**	Workload	✓	✓	✓
9.0	**Number of Non-Resolvable Contacts Assigned to Resolver Groups**	Channel Efficacy	✓	✓	✓
10.0	**Number of Resolvable Contacts Assigned to Resolver Groups**	Performance Indicator	✓	✓	✓
11.0	**Number of Contacts Resolved at First Contact**	Workload	✓	✓	✓
11.1	First Contact Resolution	Performance Indicator	✓	✓	✓
12.0	**Total Number of Resolvable Contacts [9.0 + 10.0 + 11.0]**	Workload	✓	✓	✓
13.0	**Number of Out-of-Scope Contacts**	Channel Efficacy	✓	✓	✓
14.0	**Existing Tickets: Re-direct Due to Incorrect Original Assignment (Bouncing Tickets)**	Performance Indicator	✓	✓	✓
15.0	**Existing Tickets: Request for Status**	Performance Indicator	✓	✓	✓
16.0	**Second Ticket Opened: Tagged to Existing Ticket not Resolved (Issue Persists)**	Performance Indicator	✓	✓	✓
17.0	**New Tickets Opened: Request Fulfilment**	Workload	✓	✓	✓
18.0	**New Tickets Opened: Incident Management**	Workload	✓	✓	✓
19.0	**New Tickets Opened: Request for Change**	Workload	✓	✓	✓
20.0	**Total Number of Interactions* [13.0 + 14.0 + 15.0 + 16.0 + 17.0 + 18.0 + 19.0]**	Workload	✓	✓	✓
21.0	**Opening Backlog of Service Requests**	Workload	✓	✓	✓

	Key Performance Indicator	Category	Daily	Weekly	Monthly
22.0	**New Tickets Opened: Request Fulfilment**	Workload	✓	✓	✓
23.0	**Service Requests Processed**	Performance Indicator	✓	✓	✓
24.0	**Closing Backlog of Service Requests [21.0 + 22.0 - 23.0]**	Performance Indicator	✓	✓	✓
24.0	**New Tickets Opened: Request Fulfilment Volume by Type/Category**	Workload	✓	✓	✓
25.0	**New Tickets Opened: Incident Management Volume by Type/Category**	Workload	✓	✓	✓
26.0	**New Tickets Opened: Request for Change Volume by Type/Category**	Workload	✓	✓	✓
27.0	**Number of Outbound Calls for Additional Information**	Enterprise Issues	✓	✓	✓
28.0	**Issues Impacting Delivery of Service - Non-excusable Events**	Performance Indicator	✓	✓	✓
29.0	**Issues Impacting Delivery of Service - Excusable Events**	Enterprise Issues	✓	✓	✓
30.0	**Root Cause Analysis of High Contact Volume Periods**	Enterprise Issues	✓	✓	✓
31.0	**Root Cause Analysis for Periods of High Backlog for Service Requests**	Performance Indicator	✓	✓	✓
32.0	**Customer Satisfaction**	Performance Indicator	-	-	✓
33.0	**Quality Assurance**	Performance Indicator	-	-	✓

Line 8.0 Total Number of Contacts and Line 19.0 Total Number of Interactions must be reconciled if different

Any changes to reporting required by SSC which results in the development or modification of reporting tools will be provided at no cost to SSC.

3.2 EUSD KPI Report Content

For each of the five End User Customers, the Contractor shall prepare, in soft copy form, KPI Reports containing the following analytic data, for the intervals indicated:

Table 93: EUSD KPI Reporting

	Key Performance Indicator	Category	Daily	Weekly	Monthly
1.0	**Number of Abandoned Calls**	Workload	✓	✓	✓
1.1	Calls Abandoned in 60 seconds or less	Workload	✓	✓	✓
1.2	Calls Abandoned in greater than 60 seconds	Workload	✓	✓	✓
1.3	Average Time to Abandon Call	Performance Indicator	✓	✓	✓
1.4	Call Abandonment Rate	Performance Indicator	✓	✓	✓
2.0	**Number of Calls Answered by Service Desk Agents**	Workload	✓	✓	✓
2.1	Average Wait Time	Performance Indicator	✓	✓	✓
2.2	Average Talk Time	Performance Indicator	✓	✓	✓
2.3	Average Handle Time (including wrap-up)	Performance Indicator	✓	✓	✓
2.4	Percentage of Calls Answered in Base Target: 45 seconds or less	Performance Indicator	✓	✓	✓
2.5	Percentage of Calls Answered in Ceiling Target: 120 seconds or less	Performance Indicator	✓	✓	✓
2.6	Month-to-Date Percentage of Calls Answered in Base Target: 45 seconds or less	Performance Indicator	✓	-	-
2.7	Month-to-Date Percentage of Calls Answered in Ceiling Target: 120 seconds or less	Performance Indicator	✓	-	-
3.0	**Number of Abandoned Chats**	Workload	✓	✓	✓
3.1	Chats Abandoned in 60 seconds or less	Workload	✓	✓	✓

	Key Performance Indicator	Category	Daily	Weekly	Monthly
3.2	Chats Abandoned in greater than 60 seconds	Workload	✓	✓	✓
3.3	Average Time to Abandon Chat	Performance Indicator	✓	✓	✓
3.4	Chat Abandonment Rate	Performance Indicator	✓	✓	✓
4.0	**Number of Chats Answered by Service Desk Agents**	Workload	✓	✓	✓
4.1	Average Wait Time	Performance Indicator	✓	✓	✓
4.2	Average Chat Time	Performance Indicator	✓	✓	✓
4.3	Average Handle Time (including wrap-up)	Performance Indicator	✓	✓	✓
4.4	Percentage of Chats Answered in Base Target: 45 seconds or less	Performance Indicator	✓	✓	✓
4.5	Percentage of Chats Answered in Ceiling Target: 120 seconds or less	Performance Indicator	✓	✓	✓
4.6	Month-to-Date Percentage of Chats Answered in Base Target: 45 seconds or less	Performance Indicator	✓	-	-
4.7	Month-to-Date Percentage of Chats Answered in Ceiling Target: 120 seconds or less	Performance Indicator	✓	-	-
5.0	**Number of Emails Deemed Not Actionable***	Channel Efficacy	✓	✓	✓
6.0	**Number of Emails Responded by Service Desk Agents (without automation)***	Workload	✓	✓	✓
6.1	Percentage of Emails Responded within Base Target: 1 hour or less*	Performance Indicator	✓	✓	✓
6.2	Percentage of Emails Responded within Ceiling Target: 4 hours or less*	Performance Indicator	✓	✓	✓
6.3	Month-to-Date Percentage of Emails Responded within Base Target: 1 hour or less*	Performance Indicator	✓	-	-
6.4	Month-to-Date Percentage of Emails Responded to within Ceiling Target: 4 hours or less*	Performance Indicator	✓	-	-
7.0	**Number of Self-Service Portal Requests Responded by Service Desk Agents****	Workload	✓	✓	✓
7.1	Percentage of Self-Service Portal Requests Responded within Base Target: 1 hour or less**	Performance Indicator	✓	✓	✓
7.2	Percentage of Self-Service Portal Responded within Ceiling Target: 4 hours or less**	Performance Indicator	✓	✓	✓
7.3	Month-to-Date Percentage of Self-Service Portal Requests Responded within Base Target: 1 hour or less**	Performance Indicator	✓	-	-
7.4	Month-to-Date Percentage of Self-Service Portal Requests Responded within Ceiling Target: 4 hours or less**	Performance Indicator	✓	-	-
8.0	**Total Number of Contacts[Note] [2.0 + 4.0 + 6.0 + 7.0]**	Workload	✓	✓	✓
9.0	**Number of Non-Resolvable Contacts Escalated to the Enterprise Service Desk [EUSD Only]**	Channel Efficacy	✓	✓	✓
10.0	**Number of Resolvable Contacts Escalated to the Enterprise Service Desk [EUSD Only]**	Performance Indicator	✓	✓	✓
11.0	**Number of Contacts Resolved at First Contact**	Workload	✓	✓	✓
11.1	First Contact Resolution	Performance Indicator	✓	✓	✓
12.0	**Total Number of Resolvable Contacts [9.0 + 10.0 + 11.0]**	Workload	✓	✓	✓
13.0	**Number of Out-of-Scope Contacts**	Channel Efficacy	✓	✓	✓
14.0	**Existing Tickets: Re-direct Due to Incorrect Original Assignment (Bouncing Tickets)**	Performance Indicator	✓	✓	✓
15.0	**Existing Tickets: Request for Status**	Performance Indicator	✓	✓	✓
16.0	**Second Ticket Opened: Tagged to Existing Ticket not Resolved (Issue Persists)**	Performance Indicator	✓	✓	✓
17.0	**New Tickets Opened: Request Fulfilment**	Workload	✓	✓	✓
18.0	**New Tickets Opened: Incident Management**	Workload	✓	✓	✓
19.0	**Total Number of Interactions[Note] [13.0 + 14.0 + 15.0 + 16.0 + 17.0 + 18.0]**	Workload	✓	✓	✓
20.0	**Opening Backlog of Service Requests**	Workload	✓	✓	✓
21.0	**New Tickets Opened: Request Fulfilment**	Workload	✓	✓	✓
22.0	**Service Requests Processed**	Performance Indicator	✓	✓	✓
23.0	**Closing Backlog of Service Requests [20.0 + 21.0 - 22.0]**	Performance Indicator	✓	✓	✓
24.0	**New Tickets Opened: Request Fulfilment Volume by Type/Category**	Workload	✓	✓	✓
25.0	**New Tickets Opened: Incident Management Volume by Type/Category**	Workload	✓	✓	✓

	Key Performance Indicator	Category	Daily	Weekly	Monthly
26.0	**Number of Outbound Calls to Confirm Service Restoration**	Workload	✓	✓	✓
27.0	**Issues Impacting Delivery of Service - Non-excusable Events**	Performance Indicator	✓	✓	✓
28.0	**Issues Impacting Delivery of Service - Excusable Events**	Enterprise Issues	✓	✓	✓
29.0	**Root Cause Analysis of High Contact Volume Periods**	Enterprise Issues	✓	✓	✓
30.0	**Root Cause Analysis for Periods of High Backlog for Service Requests**	Performance Indicator	✓	✓	✓
31.0	**Customer Satisfaction**	Performance Indicator	-	-	✓
32.0	**Quality Assurance**	Performance Indicator	-	-	✓

Note: Line 8.0 Total Number of Contacts and Line 19.0 Total Number of Interactions must be reconciled if different
* Only applies to Health Canada (HC)
** Does not apply to Health Canada (HC)

Any changes to reporting required by SSC which results in the development or modification of reporting tools will be provided at no cost to SSC.

3.3 KPI Reporting Deadlines

The Contractor will provide periodic KPI reports, in the prescribed format, in accordance with the following timelines:

3.3.1 Daily KPI Reporting

The Contractor will provide daily KPI reports within one (1) FGWD.

3.3.2 Weekly KPI Reporting

The Contractor will provide weekly KPI reports within one (1) FGWD following the completion of the reporting period.

3.3.3 Monthly KPI Reporting

The Contractor will provide monthly KPI reports within five (5) FGWDs following the completion of the reporting period. Monthly reports should include columns for (i) current data, (ii) prior month and (iii) variance (current month minus prior month).

4.0 Network Performance Reporting

The Contractor will continuously monitor and measure their network and internet connection to ensure that it is operating as needed to meet Service Level Requirements. The format for reporting Network Performance is described in **Schedule A 8 – System and Network Architecture** and re-produced here:

4.1 Network Performance Reporting Window

The Contractor will report on the Network Performance for each month of the Contract Term.

4.2 Network Performance Reporting Deadline

Within five (5) Federal Government Working Days (FGWD) after the end of each month, the Contractor will provide a Network Performance Report, in the prescribed manner.

4.3 Network Performance Report Content

At a minimum, the Network Performance Report must include the following:

(a) Internet utilization at an hourly average and peak;

(b) Latency experienced between the provider and SSC service;

(c) Network packet loss and network jitter

(d) Experienced network speed;

(e) Quality of service rules in place to prioritize the service desk traffic over other traffic. The report must indicate: (i) the quality of service rules in place, and (ii) when settings were changed during the month; and

(f) Observations and any remedial actions the vendor will undertake to ensure the services to SSC are being met.

5.0 Report Repository

SSC shall provide a secure common repository for storage and retention of all SLR reports, KPI reports and Network Performance Reports. The Contractor shall be responsible for uploading and organizing reports to the common drive in accordance with the respective reporting deadlines detailed in Section 2.3 SLR Reporting Deadlines, Section 3.3 KPI Reporting Deadlines, and Section 4.2 Network Performance Reporting Deadline above.