December 1, 2016

The Honourable Kevin Sorenson, P.C., M.P.
Chair
Standing Committee on Public Accounts
House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Sorenson:

Further to the letter of September 29, 2016, from the Honourable Judy M. Foote, Minister of Public Services and Procurement, in which she provided the Government of Canada's response to the Standing Committee on Public Accounts' report entitled Report 4—Information Technology (IT) Shared Services—from the 2015 Fall Reports of the Auditor General of Canada that was presented on June 1, 2016—I am pleased to provide the Committee with the following requested information:

- Recommendation #1: The Shared Services Canada (SSC) Service Management Strategy 2015–2018 and an update on the Strategy for 2016 (see enclosed).
- Recommendation #2: A summary of service-level expectations that SSC has put in place for the IT services it delivers to customer organizations (see enclosed).
- Recommendation #3: The IT Strategic Plan has been available on the Treasury Board of Canada Secretariat's website since June 30, 2016 (see enclosed).
- Recommendation #4: Clearly defined roles and responsibilities for the management and delivery of IT security services between SSC and government departments and agencies (the Responsible, Accountable, Consulted, Informed matrix and an explanatory guide are enclosed).
- Recommendation #5: The consultation document that outlines the proposed revised Transformation Plan was made available on September 20, 2016, and the consultation closed on November 14, 2016 (see enclosed).

.../2

As reflected in the government response to the committee recommendations, following its consideration by Cabinet, SSC's revised IT transformation plan will be provided to the Committee. The revised plan will include information regarding the Enterprise-wide Cost Management Framework and how SSC has refined its methodologies and practices to determine and report on savings, including the baseline used to calculate the savings and a list of the costs not taken into account in the calculations. Furthermore, the revised plan will contain SSC's financial benchmarks for cost savings. SSC will report annually on those benchmarks, including on any significant deviations, in its departmental performance reports:

- Recommendation #5: That by December 1, 2016, SSC provide the Standing Committee on Public Accounts (PACP) with its updated Transformation Plan, including the new timelines for the completion of the three transformation initiatives, including email, data centres, and network services. In addition, beginning with the 2016–2017 fiscal year, SSC should—no later than 30 days after the end of each fiscal year— provide PACP with an annual progress report on each of the transformation initiatives until they are completed (document to follow).

- Recommendation #6: That by December 1, 2016, SSC provide PACP with its approved Service Pricing Strategy and explain how the strategy will help SSC prioritize and allocate its funding and ensure that it has the available funding to address its deficiencies (document to follow).

- Recommendation #7: That by December 1, 2016, SSC provide PACP with a progress report outlining how SSC refined its methodologies and practices to more accurately determine and report savings to Parliament and to the public. This report should include the baseline used to calculate the savings as well as a detailed list of all of the costs borne by the federal government that were not taken into account in the calculations (document to follow).

- Recommendation #8: That going forward, SSC publish concrete financial benchmarks of cost savings that align with its annual strategic plan and that SSC report on the cost savings annually, including a full discussion of any key factors that caused a material deviation from the benchmarks (document to follow).

.../3

I trust this information responds to your request. Should you require additional information, please do not hesitate to contact me by telephone at 613-670-1777 or by email at ron.parker@canada.ca.

Sincerely,

Ron Parker
President

c.c. The Honourable Tom Lukiwski, P.C., M.P.
Chair of the Standing Committee on Government Operations and Estimates

Michael Ferguson
Auditor General of Canada

Caroline Massicotte
Clerk of the Standing Committee on Government Operations and Estimates

Michel Marcotte
Clerk of the Standing Committee on Public Accounts

Enclosures

SHARED SERVICES CANADA

Response to the Standing Committee on Public Accounts Report entitled: Report 4 Information Technology Shared Services of the Fall 2015 Reports of the Auditor General of Canada

TABLE OF CONTENTS

Service | Innovation | Value

SHARED SERVICES CANADA

Service Management Strategy

2015 – 2018

Version: Final

Date: December 9, 2015

Doc ID: 3018704

Shared Services Canada | Services partagés Canada

Canada

APPROVAL

The signing authority below concurs with the content specified within this document.

Executive Sponsor: SSC Deputy Head

Name:	Ron Parker, President		
Signature:	Ron Parker	Date:	14/12/15

The SSC Service Management Strategy received formal approval from the Senior Management Board on December 9, 2015.

APPROVAL

Shared Services Canada's Service Management Strategy – 2016 Annual Report

The signing authority below concurs with the content of this document.

Executive Sponsor: Shared Services Canada's Deputy Head

Name:	Ron Parker, President		
Signature:	Ron Parker	Date:	NOV 0 2 2016

Shared Services Canada's Service Management Strategy – 2016 Annual Report received formal approval from the Senior Management Board on October 12, 2016.

This document includes the original Service Management Strategy 2015 - 2018 as well as updated content from the Service Management Strategy 2016 Annual Report. Appendix A details include current status of initiatives in section 1.2 of the Service Management Strategy 2015 - 2018 (identified with *****) as well as, the identification and status of new initiatives within the Service Management Strategy 2016 Annual Report (identified with ******).

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE

To support the improvement of the Shared Services Canada (SSC) service management approach and overall delivery of its services to customers, a three (3) year departmental Service Management Strategy (SMS) has been developed. The intent of the SMS is to provide strategic direction to the department as it delivers on the service improvement initiatives and sub-initiatives identified in the table below. The SMS objective is to deliver IT Infrastructure services to the Government of Canada (GC) that are customer centric, realizes operational efficiencies and promotes a culture of service management excellence.

In addition, the SMS will demonstrate how SSC will measure and improve service performance and mitigate risks over the next three (3) years. Deputy Heads, in accordance with the TBS Policy on Service*, will be responsible for ensuring that SSC's enterprise services are customer-centric, that operational efficiencies are realized and that a culture of service management excellence is promoted within the department.

Service Improvement Initiative	Service Improvement Sub- Initiative	High Level Description
Improve Service Management Approach	Improve visibility and accessibility of services to customers	Evolve the customer-accessible view of the SSC IT Infrastructure Services Catalogue. Develop and promote a single user centric on-line portal for customers to access and order SSC services through the SSC IT Infrastructure Services Catalogue
	Establish service reviews to drive service improvement and increase the quality of services delivered to customers	Implement a systematic approach to perform post implementation service reviews to support continual service improvement with key metrics and service level expectations: ▪ Phase 1: 5 priority services ▪ Phase 2: expand across other services
	Improve service delivery to customers with the establishment of service levels that can be reported on performance measurement and drive continual service improvement	Based on service review outputs and industry best practices define and publish meaningful sets of service levels to provide details on the level of service that customers can expect from SSC: ▪ Phase 1: 5 priority services ▪ Phase 2: expand across other services
	Augment e-enablement of services (e-services) to enhance, standardize and make the service delivery more effective and efficient to customers	Identify and develop a plan for areas where the automation of service delivery (e-services) to customers would yield benefits (reduced costs, higher efficiency)
	Promote e-services by engaging customers	Engage SSC customers in the process design and delivery of e-services
Framework of Customer Satisfaction Feedback	Create a customer satisfaction feedback framework and program	Engage SSC customers in the creation and design of a customer feedback framework and program

The content above has been updated from the SMS - 2016 Annual Report:
Refer to Appendix A for details regarding initiatives and activities.

* These links are only accessible from within the Government of Canada.

Based on SSC's service inventory, the following five (5) priority services have been identified for the Phase 1 implementation of the above service improvement initiatives:

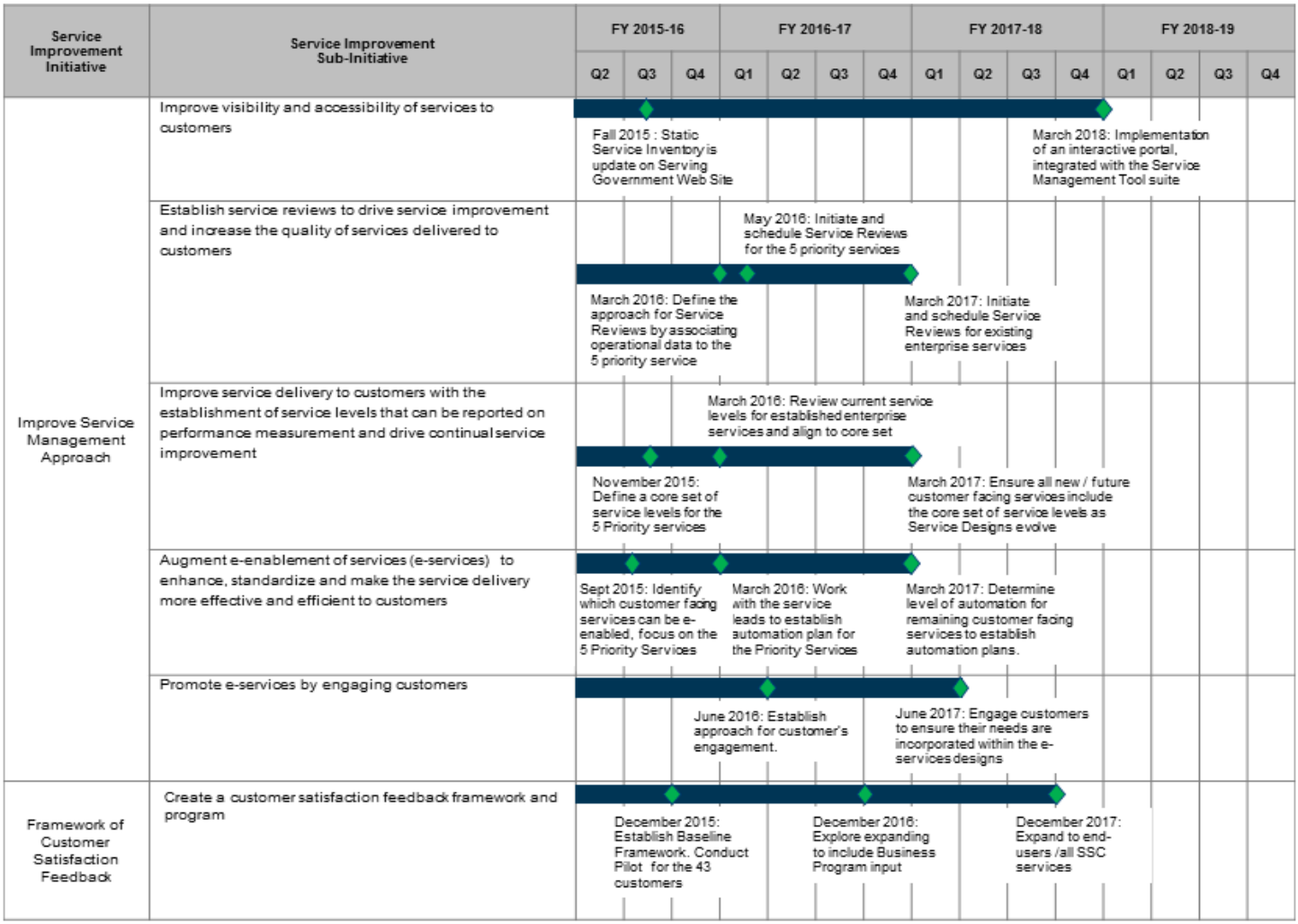
1. Email
2. Application Hosting
3. Mobile Devices
4. GCNet WAN
5. Video Conferencing

SSC's service inventory represents the list of IT Infrastructure services offered to customer departments and agencies. Although the service improvement initiatives within this SMS are focused on the five (5) priority services in Phase 1 listed above, the scope of these initiatives will be expanded in follow-on phases to include all IT Infrastructure services in the SSC Service Catalogue during the annual review of the SMS. Please see Appendix B – Service Inventory for a full list of SSC's services.

In order to achieve cost-efficiencies and demonstrate value to customers, SSC has developed a costing and pricing strategy for the delivery of SSC services. The objectives of the costing and pricing strategy are as follows:

- → Ensure fairness and transparency in the provision of IT services amongst customers;
- → Motivate customers to adopt standard service offerings;
- → Enable SSC to better manage demand for services.

1.2 KEY TIMEFRAMES



The content above has been updated from the SMS - 2016 Annual Report:
Refer to Appendix A for details regarding initiatives and activities.

1.3 GOVERNANCE

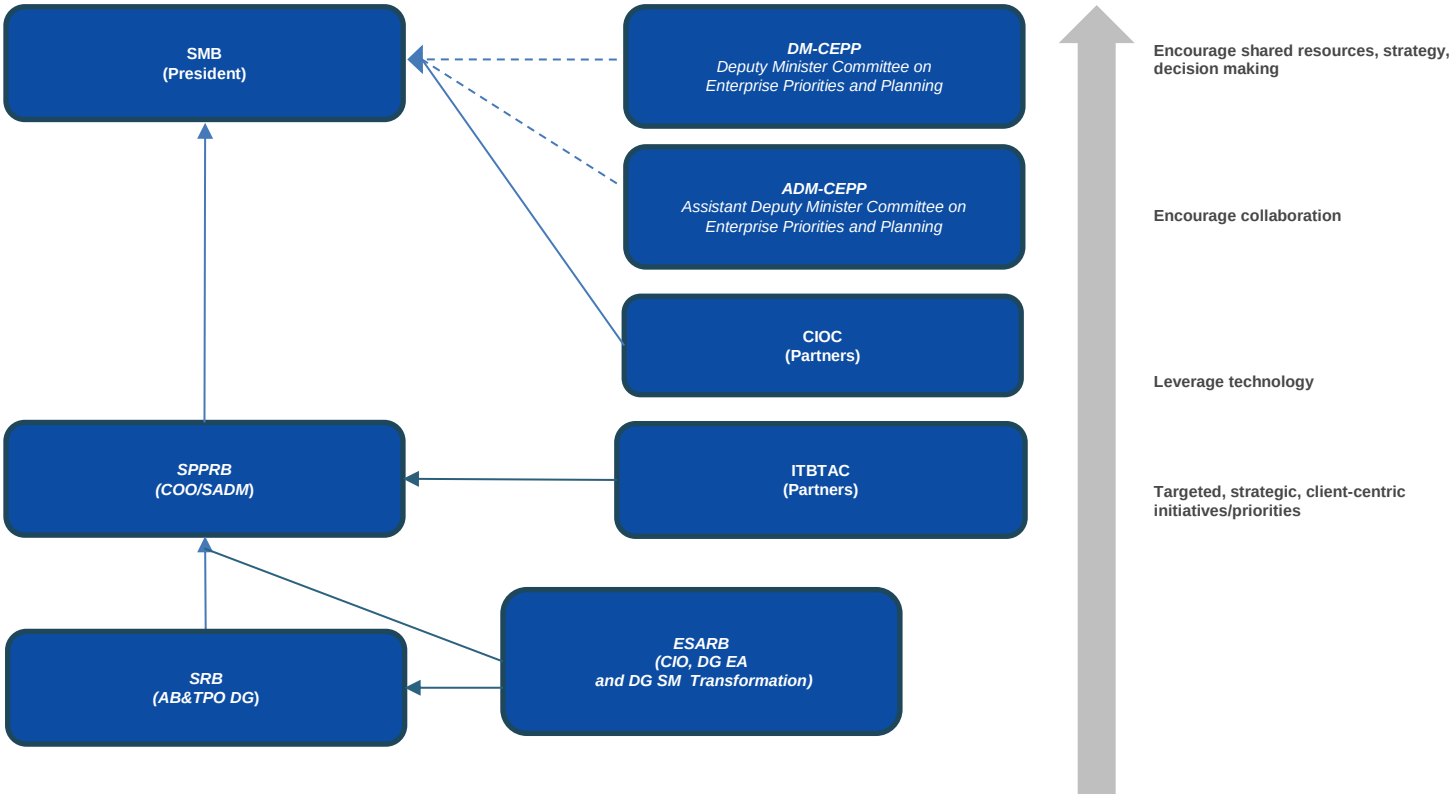
SSC governance committees through their respective mandates will review the SMS on an annual basis to ensure progressive improvement on our service management approach. SSC governance will conduct quarterly performance reviews of the service improvement initiatives as they relate to the five (5) priority services.
SSC Governance Committees are responsible for:

- → Providing guidance and oversight of SSC's service lines and critical projects to ensure alignment with SSC's strategic and service objectives;
- → Providing feedback from a government wide context on current services with an emphasis on quality improvement, timeliness, and responsiveness of all IT Infrastructure Services in the SSC Service Catalogue;
- → Monitoring progress and completion of the service improvement initiatives within the SMS ;
- → Ensuring expected results are achieved;
- → Ensuring risks are managed and performance is monitored;
- → Ensuring alignment to the TBS Policy on Service.

The content below has been updated from the SMS - 2016 Annual Report.

The Government of Canada IT Strategic Plan 2016-2020 includes two new government wide governance committees - The Deputy Minister and Assistant Deputy Minister Committees on Enterprise Priorities and Planning (CEPP) will be the governance and oversight bodies for all government IT investments. These external committees are now included in the diagram below and will manage demand from departments and agencies for SSC IT infrastructure services, and guide how SSC provides those supply-side services.

In addition, there have been three (3) changes to our internal governance committees to improve our customer-centric approach to enterprise services and demonstrate operational efficiencies to our customers .



Note: - - - - - represents external governance committees

Senior Management Board (SMB)
Chair, President

- Senior Management Board (SMB) is SSC's Senior Executive decision-making forum – full decision-making authority;
- Strategic direction, priority setting and broad oversight (i.e., "steering role");
- Sets strategic direction and enterprise-wide priorities;
- Approves corporate-wide plans, strategies, and monitoring and reporting requirements.

Service, Project and Procurement Review Board (SPPRB)
Chair, COO

- The Service, Project and Procurement Review Board's (SPPRB) key role is to provide guidance and oversight to senior management with respect to all service lines and projects, ensuring alignment with SSC's strategic and service objectives.
- The SPPRB serves as the first level of escalation for systemic service-delivery issues before referral to the Senior Management Board (SMB). Proactive efforts should be made to discuss unresolved service-delivery issues at the SPPRB before partners or clients submit formal complaints at the Deputy Minister level.

Service Review Board (SRB)
Chair, AB&TPO DG

- As a Director General (DG) sub-committee of the Service, Project and Procurement Review Board (SPPRB), the Service Review Board (SRB) has the key role of overseeing the management of Shared Services Canada's (SSC) enterprise services throughout their life cycle, including service authorization and the management of associated risk. More specifically, the SRB ensures that all elements of the service portfolio management framework that are necessary for successful service transformation are in place horizontally across the organization and are being adhered to.

Enterprise Strategies and Architecture Review Board (ESARB)
Co-Chairs, CIO, DG EA and DG SM Transformation

- The Enterprise Strategy and Architecture Review Board's (ESARB) key role is to provide advice to senior management with respect to the evolution of enterprise strategies and associated architectures, ensuring that they are aligned with Shared Services Canada's (SSC) mandate and authority and support the Government of Canada's priorities. This role includes providing SSC and its partners and clients with guidance and oversight with respect to the future vision of SSC's offerings.

DM-CEPP
Deputy Minister Committee on
Enterprise Priorities and Planning

The coordinating body for enterprise and common services to ensure the consideration of business and enterprise priorities and guide the implementation of the Government of Canada IT Strategic Plan (strategic plan) to improve service delivery for clients and Canadians.
Responsibilities

- As the coordinating body for enterprise and common services, DM CEPP will:
- Recommend enterprise and common approaches for the delivery of which government services should be adopted
- Support and enable departments and agencies to adopt enterprise solutions for consolidated services, and recommend the pace at which departments and agencies adopt enterprise IT solutions
- Guide the balance of supply and demand, and ensure investments are sustainable and add business value
- Consider recommendations on priorities and projects from the subordinate ADM-level committee(s) (i.e. ADM-CEPP)

ADM-CEPP

Assistant Deputy Minister Committee on Enterprise Priorities and Planning

The ADM Committee on Enterprise Priorities and Planning will support the PSMAC Sub-Committee on Enterprise Priorities and Planning by:

- Advising on the development and implementation of a GC-wide IT strategy and policies that reflect business and enterprise-wide priorities and that enable improved service delivery to clients and Canadians;
- Assessing the aggregate risk of the GC's IT portfolio and reviewing risk mitigation strategies;
- Developing a principles-based framework for prioritizing IT projects and balancing capacity and demand that reflects enterprise needs;
- Applying the principles-based framework as approved by the PSMAC Sub-Committee on Enterprise Priorities and Planning to make recommendations on projects that should proceed and to identify interdependencies and opportunities for integration;
- Reviewing the development, implementation and updating of a GC Integrated IT Plan;
- Proactively anticipating and resolving prioritization conflicts between major competing initiatives and determining appropriate trade-offs when required; and,
- Providing reports and recommendations to the PSMAC Sub-Committee on Enterprise Priorities and Planning on any of the above issues.

Chief Information Officer Council (CIOC)
Chair, Departmental senior officials

- The Chief Information Officer Council is a forum for consultation and information exchange on matters relating to the effective management and use of information and technology in support of program and service delivery in the Government of Canada. The Chief Information Officer (CIO) Council is made up of departmental senior officials responsible for Information Management and Information Technology in their departments.

Information Technology Business Transformation Advisory Committee (ITBTAC)
Chair, Strategy Branch SADM

- IT Business Transformation Advisory committee provides advice to SSC on issues related to the delivery of ongoing IT services;
- Ways to improve quality, timeliness and responsiveness of services, continuous improvement;
- Approaches to enhance client satisfaction and engagement.

2 SSC DEPARTMENTAL CONTEXT

2.1 SSC'S OPERATIONAL CONTEXT

SSC operates in a rapidly changing and increasingly complex Information Technology (IT) environment. Through the enhancement of enterprise IT infrastructure services, SSC continues to be aware of shifting internal and external factors to ensure its service improvement initiatives are well planned, designed, operated and managed. A key component in reaching this goal will be leveraging technology and innovative partnerships with customers as well as Industry resulting in an efficient, more effective and affordable Government.

2.2 DEPARTMENT'S MANDATE AND KEY RESPONSIBILITIES RELATED TO SERVICE

The Office of the Auditor General (OAG) report in 2010 identified that many of the information technology systems that the federal government relies on to deliver programs and services to Canadians are aging, and post a great risk to the delivery of services to Canadians. Treasury Board was tasked with creating a long term plan and a report to address the aging IT infrastructure.

The GC created SSC in 2011 to modernize how the government manages its IT infrastructure. SSC has provided the mandate to consolidate and streamline the delivery of IT infrastructure services across the GC under the Shared Services Canada. SSC has brought together people, IT resources and assets to improve the efficiency, reliability and security of the government's IT infrastructure, increase productivity across departments and agencies, and support the vision of a 21st century public service, as articulated in Blueprint 2020.

SSC is maintaining and improving IT infrastructure service delivery while renewing the government's aging IT infrastructure. In so doing, the department is:

- → Working in partnership with key public- and private sector stakeholders;
- → Adopting enterprise-wide approaches for managing IT infrastructure services; and
- → Implementing efficient and effective business management processes and services in support of its mandate.

In alignment with the departmental mandate, SSC departmental personnel, at both the executive management and employee levels, will use the SMS as a guide and roadmap to meeting key responsibilities related to the quality delivery of IT infrastructure services to its customers. Also, the SMS will guide the implementation of the initiatives resulting in an improved service management approach for the delivery of services to customer organizations and an improved user experience of SSC services.

2.3 SERVICES COVERED BY THE SERVICE MANAGEMENT STRATEGY

The content below has been updated from the SMS - 2016 Annual Report.

SSC's pursuit to improve the department's SMS is integral to meeting customer centric, efficient, and service excellence goals. Each year, SSC will update and implement the service improvement initiatives list to incrementally realize the three (3) year SMS. Service improvements outlined in Appendix A are for all SSC services and are defined in the context of both legacy and enterprise environments.

The following five (5) priority services are covered by Phase 1 of this SMS:

Priority Service	Description
Email	✓ Email service enables SSC and its customers to send and receive electronic mail messages and includes functionalities such as calendaring, task management, address book and personal contact management.
Application Hosting	✓ The Application Hosting service provides customers with a fully managed, secure, reliable and scalable multi-tier platform, including standardized application and database middleware, which allows customers to host and manage their data and business applications.
Mobile Devices	✓ The Mobile Devices service offering provides cellular phones, smartphones and cellular data devices, along with their service plans. Specialized solutions for emergency-response personnel and senior executives on travel status are also available.
GCNet WAN	✓ The Government of Canada GCNet Wide Area Network (WAN) is a fully managed network service that interconnects customer locations across metropolitan, regional, national or international boundaries. This service enables users and computers to communicate with other users and computers in other locations, while supporting business applications for simultaneous voice, data and video communications, as required.
Video Conferencing	✓ An integrated and standardized service that provides Government of Canada employees the ability to connect video enabled boardrooms and video enabled desktop endpoints between departments on the Government of Canada shared metropolitan network.

2.4 RELATIONSHIP TO OTHER DEPARTMENTAL OR GC-WIDE INVESTMENTS OR INITIATIVES

SSC contributes to the achievement of other critically important and transformational GC initiatives including the vision of the public service of the future as articulated in Blueprint 2020. In addition, SSC works collaboratively with other GC departments through creating a modern workplace to enable public servants to work in an even more effective way, in alignment with Government of Canada's Workplace 2.0 initiative. These GC initiatives contribute to SSC's long term SMS and its commitment to customer service management excellence.

BLUEPRINT 2020

The GC is asking departments to reduce costs by finding efficient, interconnected and nimble processes, structures and systems. Government needs to work smarter - leverage new technologies. Working together with customers, SSC needs to make smart use of new technologies and achieve the best possible outcomes. Blueprint 2020 is a vision of a modern and world class public service equipped to serve Canada and Canadians. SSC will support Blueprint 2020 through the Transformation Plan as an organization dedicated to implementing a whole-of-government approach to the challenges of IT in the 21st century.

Government-Wide Context

In a government-wide context, SSC is leading on four signature initiatives, as highlighted in Blueprint 2020: Government Electronic Directory Services (GEDS) 2.0, expanded availability of Wi-Fi, tools to support a mobile workforce, and desktop videoconferencing.

SSC is also working with the Treasury Board Secretariat (CIO Branch) on open access into departmental intranet sites and enhancements to Government of Canada social media (GCpedia and GCconnex) within SSC.
SSC submitted its departmental Blueprint 2020 interim report in October 2013 and its Progress Report and Action Plan in March 2014. Shortly thereafter, SSC launched several departmental initiatives, including the Innovation Fund, the Crowdsourcing Tool, the Mentorship Program, and The Academy. With an eye to the future, SSC will continue to engage employees and colleagues to refine existing initiatives and seek out new ones to keep abreast of our constantly changing society. These initiatives roll up to promote and further the overall vision and mandate of SSC and its overall SMS objectives.

Workplace 2.0

SSC and Public Works & Government Services Canada (PWGSC) are partnering to finalize a Memorandum of Understanding that will determine a governance structure, roles and responsibilities, collaboration, participation and innovation on fit-up projects, and including SSC's standards in the GC Workplace 2.0 fit-up GC Workplace standards. The initiative aims to create a modern workplace that will attract, retain and encourage public servants to work smarter, greener and healthier to better serve Canadians. Workplace 2.0 consists of three pillars of renewal:

SSC is also supporting the government wide initiative of open government where the GC is aiming to maximize the release of government information to support transparency, accountability, citizen engagement, and socio-economic benefits through reuse, subject to applicable restrictions associated with privacy, confidentiality, and security. The expected results of open government:

- → Canadians are able to find and use Government of Canada information and data to support accountability, to facilitate value-added analysis, to drive socio-economic benefits through reuse, and to support meaningful engagement with their government.
- → Alignment with overall objectives of the Service Management Strategy.

3 DEPARTMENTAL SERVICE VISION

The content below has been updated from the SMS - 2016 Annual Report.

SSC's vision is to provide modern, reliable, secure and cost-effective IT infrastructure services to support government priorities and program delivery.

SSC is committed to meeting the needs of its customers through improving its service management approach;
SSC's vision for service applies to all services, including legacy and enterprise services. Budget 2016 included additional funding for SSC to maintain legacy equipment as the transition to enterprise services is ongoing. An ongoing evergreening strategy for all services is being developed as part of SSC's Transformation Plan reset in fall 2016.

The SMS reflects SSC's overall vision to:

- → provide customer-centric, cost-effective shared services that improve service delivery;
- → improve the customer experience, increase efficiencies, and reduce delivery costs; and
- → provide best value to customers.

SSC is dedicated to demonstrating results and realizing cost efficiencies through the transformation of Government of Canada IT infrastructure services. We have taken a collaborative approach by engaging customers to participate in a delivery-cost-reduction exercise to reduce the overall costs of SSC services.

To achieve the service vision, SSC must be in constant engagement with its stakeholders for the planning, design and delivery of SSC's service inventory. The service improvement initiatives outlined in Appendix A demonstrates the department's commitment to ensuring that the priorities are at the forefront of how SSC will meet its vision and objectives. A critical enabler of supporting how SSC addresses the priorities will be to leverage existing and emerging service trends.

4 DEPARTMENTAL SWOT ANALYSIS

The identified strengths, weaknesses, opportunities and threats were developed through consultation with SSC stakeholders and serve as key inputs into the development of the SMS and its related service improvement intiatives. Through the provision of services and implementation of the SMS, SSC will remain aware of the identified strengths and opportunities, while acknowledging the risks posed by the weaknesses and threats.

An environmental scan of the department's internal and external factors are an intregal part of the SMS as well as the departmental strategic planning and prioritization process. Environmental factors internal to SSC, are usually classified as Strengths (S) or Weaknesses (W) and those external to the organization as Opportunities (O) or Threats (T). The following SWOT analysis provides information on the alignment with SSC's vision:

The content below has been updated from the SMS - 2016 Annual Report.

The SWOT analysis has been updated to take into consideration the recommendation from The Fall 2015 Report from the Office of the Auditor General (OAG) and the results of the Customer Satisfaction Surveys http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback/monthly-results* concerning timeliness, positive outcomes and process aspects.

* These links are only accessible from within the Government of Canada.

Strengths	Weaknesses	Opportunities	Threats
An organization's strengths are its resources and capabilities that can be used for developing competitive advantage.	The absence of certain strengths may be viewed as weaknesses or, in this case, the gap between what SSC aspires to be and its current level of service management process and organizational maturity.	The external environmental analysis may reveal new opportunities for excellence or growth.	Changes in the external environment may also present threats to the organization.
1.0) Strong support for Service Management evolution and improvement from President, COO and Executive Leadership Team.*	1.0) Service Management evolution and improvement plans are evolving, have not been fully communicated and/or are not fully accepted across the Department.*	1.0) Implement the SMS and ensure that the service improvement plans are widely communicated and understood across the organization.* 1.1) Leverage the GC IT prioritization committees to ensure alignment.*	*1.0) Departmental service priorities could be impacted by potential legislative and/or other GC priorities.**
**Note: Strength, Weakness, Opportunity and Threat analysis 1.0 has been addressed as follows:* *SSC's SMS has been communicated across the organization through official communications as well as published on the My SSC portal. Service improvement plans have been communicated and are understood across the organization. All actions for this opportunity have been completed.*			
2.0) Recent reorganization (April 1, 2015) of SSC around lines of service enables a more service- and customer-centric approach to the delivery of services.*	2.0) Customer expectations are not well understood by the lines of service.*	2.0) Develop service levels that will satisfy customer expectations within acceptable costs to GC.*	2.0) Lack of appropriate customer participation.*
**Note: Strength, Weakness, Opportunity and Threat analysis 2.0 has been addressed as follows:* *Service levels have been completed and are posted on the SSC Service Catalogue*, which is available on both the My SSC and Serving Government portals. All actions for this opportunity have been completed.*			

3.0) Strong understanding of technology within the lines of service.*	3.0) End-to-end Service Management is not fully understood within the lines of service. Focus is primarily on technical components.*	3.0) Establish a service review that will provide a holistic review of service performance from a customer request through to SSC fulfilment.*	3.0) A mismatch between the customer's view of service quality and SSC's view.*

**Note: Strength, Weakness, Opportunity and Threat analysis 3.0 has been addressed as follows:*
A formal service review process has been developed and approved. All SSC services are scheduled for formal review at least once during the period covered by the strategy. All actions for this opportunity have been completed.

4.0) Service inventory, established ownership, accountability and responsibility for each service are assigned.	4.0) Service Information within the SSC service portal is largely IT-focused and is not presented in customer service business terms.	4.0) Enhance SSC's single-service portal by providing appropriate service information and ensuring a quality e-enabled experience for customers.	4.0) Inability to satisfy customer needs.
5.0) Formal customer engagement is established at the COO and Executive Leadership Team levels through the IT Service Management Advisory Committee (ITSMAC), the **IT Business Transformation Advisory Committee (**ITBTAC) and the Chief Information Officer Council (CIOC).*	5.0) A formal mechanism to monitor and measure customer feedback on the performance and management of the services has not been implemented.*	5.0) Establish a formal customer satisfaction mechanism in order to monitor and measure the performance and management of services and identify areas for improvement.*	5.0) Lack of appropriate customer participation.*

**Note: Strength, Weakness, Opportunity and Threat analysis 5.0 has been addressed as follows:*
A formal customer satisfaction mechanism has been developed and approved. The results are available on the SSC Serving Government portal located at http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback. All actions for this opportunity have been completed.*

6.0) Recent reorganization (August 18, 2016) of SSC's Service Delivery and Management organization has increased leadership capacity to focus on customer-centric service delivery and Enterprise Business Intake and Demand Management (EBIDM).	*6.0) Multiple channels of customer business intake are still possible.*	*6.0) Mature the enterprise business intake and demand management processes, allowing for better management of demand and service delivery in support of customer needs and expectations.*	*6.0) Lack of appropriate customer participation.*
7.0) Service Level Expectations are defined for all SSC Services and are included within the Service Catalogue.	*7.0) Service Standards guidelines are not fully understood.*	*7.0) Refine the framework and approach aligning to TBS Service Standards guidelines.*	*7.0) Departmental service priorities could be impacted by potential legislative and/or other GC priorities.**

* These links are only accessible from within the Government of Canada.

5 SERVICE IMPROVEMENT OBJECTIVES AND INTIATIVES

5.1 SERVICE IMPROVEMENT OBJECTIVES

The service improvement objectives are driven by SSC's mandate and vision and aligned to the TBS Policy on Service principles. Service excellence is about engaging our staff to focus on our customer's needs, while nurturing the qualities that contribute to a culture of continuous improvement in the pursuit of SSC departmental excellence. This is achieved by ensuring that our staff, processes, and innovative technologies are aligned to help us work together to meet the needs of our customers. To meet service excellence objectives while ensuring alignment with the TBS Policy on Service principles, the implementation of the service improvement initiatives will meet the following objectives:

- → Highlight service stewardship, enterprise alignment, and customer-centric service;
- → Enhance how customers access SSC services via the portal;
- → Improve the customer experience, increase efficiencies;
- → Priorities and initiatives identified are in alignment with the TBS Policy on Service principles;
- → Demonstrate service excellence, innovation and value for money by:
    - → Sharing an enterprise mindset and culture of service excellence;
    - → Preparing for the future state of SSC;
    - → Representing a holistic structural model of the future; and
    - → Ensuring readiness for broader GC initiatives.
- → Measurably strengthen program/project management and service delivery;
- → Continue to improve and increase capacity to deliver online, e-services by:
    - → Integrate and optimize service delivery channels to provide consistent quality services and information;
    - → Leverage existing investments in technology to increase automation and online service delivery while ensuring privacy and security.

SSC employees all play a role in achieving service excellence by applying these guiding principles:

1. Self Service by Design: Enable customers to carry out select services (e-services) themselves.
2. Standardized, Streamlined with End-to-End Integration: Foster a culture of "One SSC" through an integrated single access point (portal) offering standardized workflow driven business processes enabled by technology on a shared and common infrastructure.
3. Managed Service Delivery Operation: Apply customer service delivery practices to operations and management to ensure that the capacity to deliver is in place ahead of demand. Set service and cost levels and provide fit-for-purpose services.

5.2 SERVICE IMPROVEMENT INITIATIVES

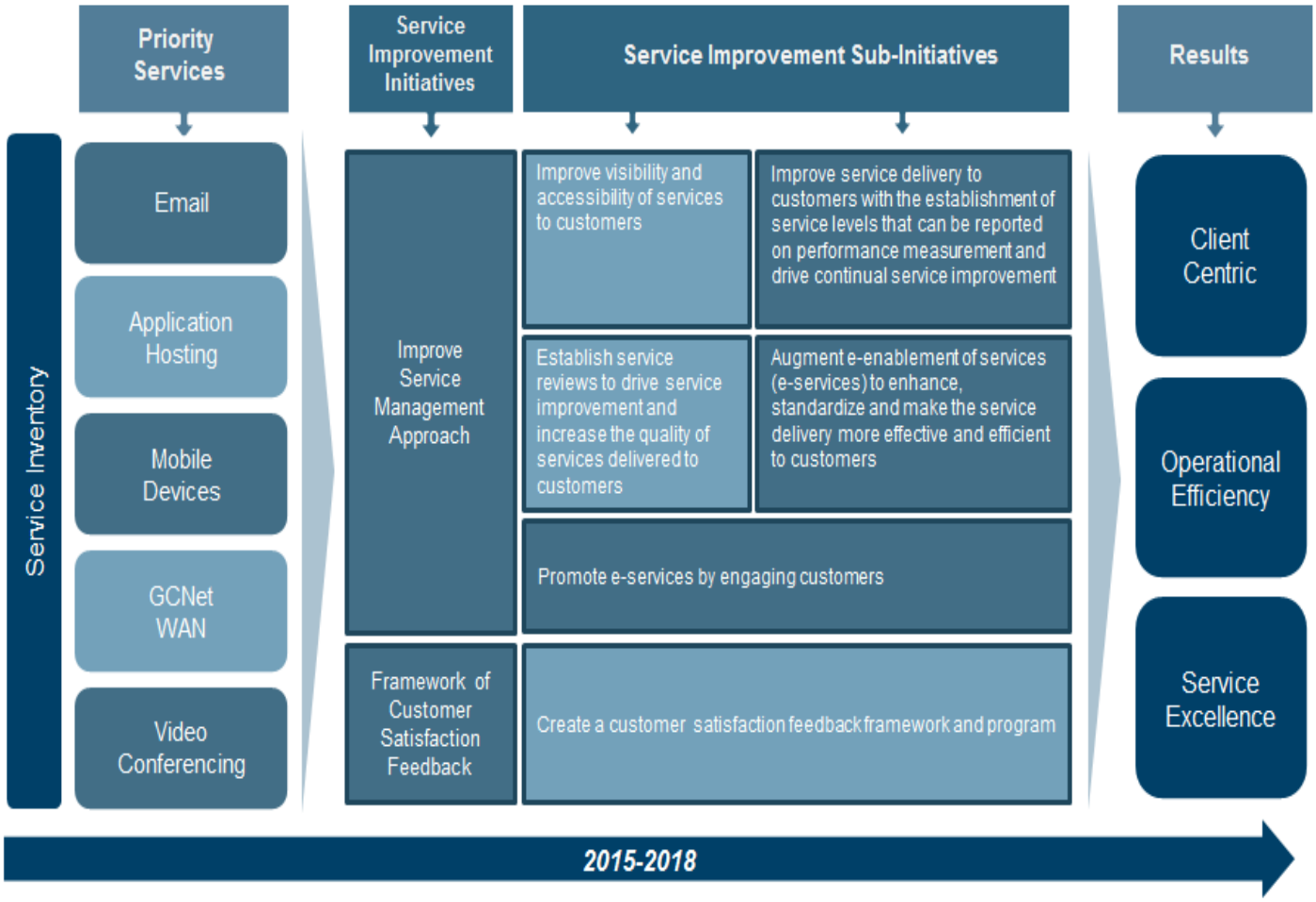
SSC seeks to improve the service management approach and create a customer satisfaction feedback framework and program as the service improvement initiative in support of the departmental SMS.

The content below has been updated from the SMS - 2016 Annual Report, refer to Appendix A.
Over the past year, significant progress has been made, and in some cases activities have been completed ahead of schedule, allowing for new initiatives to be identified. For updates on existing initiatives, refer to Appendix A.

The table below lists the service improvement initiatives and sub initiatives related to SSC's approach to improve service management and customer feedback illustrating how the initiatives link to the Policy on Service:

Service Improvement Initiative	Service Improvement Sub-Initiative	Expected Results/Objectives	Link to TBS Policy on Service
Improve Service Management Approach	Improve visibility and accessibility of services to customers	• Provide clear information on service definition and standards • Improve organization/structure of service information to be more user centric	• Client–Centric Service • Operational Efficiency • Culture of Service Management Excellence
	Establish service reviews to drive service improvement and increase the quality of services delivered to customers	• Identify and resolve tactical and strategic service related issues and risks, in collaboration with the appropriate authority to drive improvements Incorporates: • Service performance metrics • Customer satisfaction • Service cost	• Operational Efficiency • Culture of Service Management Excellence
	Improve service delivery to customers with the establishment of service levels that can be reported on performance measurement and drive continual service improvement	• Further develop published service definition; including service levels • Establish Key Performance Indicators to enhance performance measurement capabilities • Communicate the service level results with stakeholders	• Client–Centric Service • Operational Efficiency • Culture of Service Management Excellence
	Augment e-enablement of services (e-services) to enhance, standardize and make the service delivery more effective and efficient to customers	• Streamline service provisioning by maximizing automation in the delivery of SSC services to customers where feasible • Improve user experience by providing on-line self service capabilities	• Client–Centric Service • Operational Efficiency • Culture of Service Management Excellence
	Promote e-services by engaging customers	• Engage SSC customers in the process design and delivery of e-services	• Client–Centric Service • Operational Efficiency • Culture of Service Management Excellence
Framework of Customer Satisfaction Feedback	Create a customer satisfaction feedback framework and program	• Improve user experience of SSC services, internal and external processes and customer engagement and relationship management practices	• Client–Centric Service • Operational Efficiency • Culture of Service Management Excellence

Included below is a roadmap illustrating how the five (5) priority services within SSC's service inventory align to the service improvement intiatives and will result in the strategic objectives and targets of the SMS being realized.



The content above has been updated from the SMS - 2016 Annual Report. For more details refer to Appendix A.

New Initiatives

E-enablement

In alignment with the Policy on Service requirement 7.9 effective October 1, 2016, the Department must ensure that the proportions of internal enterprise services are e-enabled and that clear targets for increasing the proportion of e-services are established. To this end, the e-enablement of services is now a separate initiative to ensure proper focus and monitoring of this key policy requirement. The initiative identifies key deliverables that must be put in place prior to the establishment of the targets in 2016–2017. For further details on this service improvement initiative, refer to Appendix A.

Service Standards

The MAF 2015–2016 Departmental Report identified the need to further refine the overall approach to service performance reporting, including increasing the comprehensiveness and the consistency of, and improving client access to, service standards and related performance information. To this end, the initiative will refine the framework and approach to Service Standards and performance reporting, ensuring alignment with the Treasury Board Secretariat guideline on Service Standards, in accordance with the Policy on Service. For further details on this service improvement initiative, refer to Appendix A.

Enterprise Business Intake and Demand Management (EBIDM)

The Customer Satisfaction Feedback Initiative (CSFI) has issued surveys to chief information officers (CIOs) in our customer organizations since December 2015, and the results of the surveys can be found at http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback*. The Enterprise Business Intake and Demand Management (EBIDM) initiative was created as a result of the feedback concerning timeliness, positive outcomes, and process aspects (http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback/trends-driver*) received from the surveys. This initiative will provide a centralized enterprise approach to managing SSC demand from intake to delivery. For further details on this service improvement initiative, refer to Appendix A.

* These links are only accessible from within the Government of Canada.

6 COMMUNICATIONS AND ENGAGEMENT

SSC has identified communications and engagement as key elements of its Service Management Strategy, consisting of ongoing communications with customer organizations; integrating communications principles into service design and delivery; communicating changes to services; promoting services; and seeking feedback.

Customers: SSC believes that customer engagement involves broad input to ensure we are considering, responding to and meeting the needs of all customers. The exchange of information and ideas about SSC services is achieved through a number of channels which include, but are not limited to, CIO Forums, communiques to CIOs, messages to Deputy Heads, interaction with SSC Account Management teams, interdepartmental committees and working groups, and SSC's Serving Government website. We are committed to the following communication and engagement principles:

Integrating Communications Principles into Service Design and Delivery: During the design of services, SSC seeks a full understanding of end user preferences and requirements in order to determine how our services are presented and delivered. By understanding the target audience for SSC services, including customer readiness and the impact of any changes introduced to these audiences, the services can be designed to maximize the likelihood of a successful user experience. Through ongoing two-way communications with customers, the SSC Service Leads are positioned to determine strategies to deliver information effectively.

Informing SSC: As services are designed and delivered across the GC, it is also important to inform SSC staff about the progress of service improvement initiatives. Collaboration across SSC is crucial to share information about SSC services and to provide opportunities for SSC staff to highlight best practices, coordinate key activities and work together to overcome common organizational challenges.

Promoting Our Services: SSC's communications strategies identify the appropriate tools, messages and activities to reach target audiences in order to inform them about IT services. SSC also promotes the SSC Service Catalogue as a central portal for all customer organization services, and as a key component of the information and resources available to all public servants on the SSC Serving Government extranet site.

Feedback: SSC's communications and engagement planning is informed by input from customers across the GC. SSC works collaboratively with customers to obtain feedback on its communications activities, to identify lessons learned and to integrate innovation and best practices into future activities. This feedback may be gathered through discussions with customers involved in the communication of SSC services and/or through the use of questionnaires and surveys with stakeholders or service users.

7 PERFORMANCE FRAMEWORK

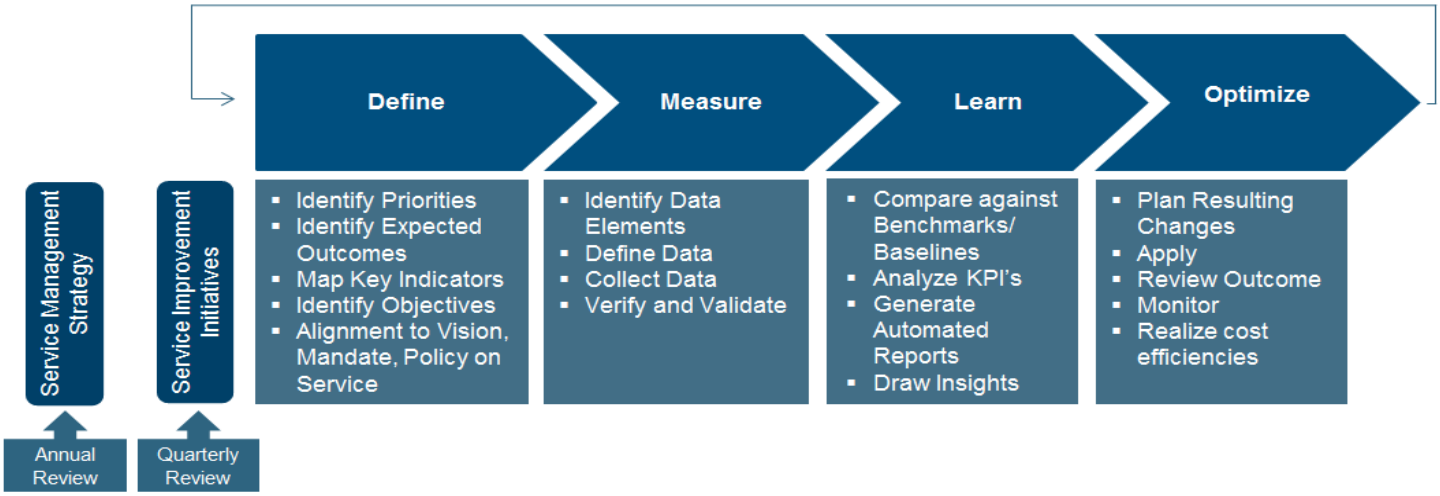
7.1 PERFORMANCE MEASUREMENT PLAN

SSC has a defined direction, including clear responsibilities and accountabilities which enable and support a performance measurement culture where managers and employees are guided to execute evidence-based informed decision-making in alignment with the Departmental Performance Report (DPR), the Report on plans and priorities (RPP), program objectives, service improvement initiatives, delivering cost-effective services, expected results, and corporate priorities.

In order to measure service delivery performance across the organization, the following six (6) principles must be followed to help guide the process:

1. Outcomes and results must be specific, measurable, assignable, realistic, time - related;
2. The performance measurement system, including data collection, should be simple and cost-effective;
3. Performance of increased cost-efficiencies realized through decreasing unit costs of services;
4. The performance measurement system should be positive;
5. Performance indicators should be simple, valid, reliable, and relevant to the activity being measured; and
6. Performance indicators will be reviewed and improved on an ongoing basis. It is only by gaining experience measuring performance that you can really refine and improve the process.

SSC will ensure an annual review of the SMS and a quarterly review of the performance of the service improvement initiatives outlined in the SMS. This will promote transparency, monitoring and continuous alignment to established initiative outcomes. These quarterly reviews will also allow the department to monitor, and ensure service improvements are on track as well as enable SSC to re-align or provide increased support for initiatives that may be off track. The following methodology will be applied in both the annual reviews of the SMS and quarterly reviews of the service improvement initiatives:



7.2 EVALUATION APPROACH

The evaluation approach for measuring performance against the service improvement initiatives will be completed and reported through performance report cards. The evaluation criteria are defined by a color coding system, presenting the overall status of each respective initiative. The results of the evaluation are determined after an assessment of the implementation target and implementation challenges, assessing whether the implementation targets will be achieved.
Legend – colour coding is:

Green: Implementation target will be achieved on target or ahead of schedule.
Yellow: Implementation target at risk. Corrective action required to protect critical path of the target.
Red: Implementation target may need to be delayed.

The content below has been updated from the SMS - 2016 Annual Report.

7.3 Performance Monitoring, Reporting and Recalibration

In 2016, we monitored service performance by means of ongoing monthly operational performance reviews (OPR) by the senior management committee, the quarterly release of an IT systems health report for partners (http://service.ssc-spc.gc.ca/en/aboutus/partners/partwork/it-health/rep2*) and monthly and annual customer satisfaction surveys.

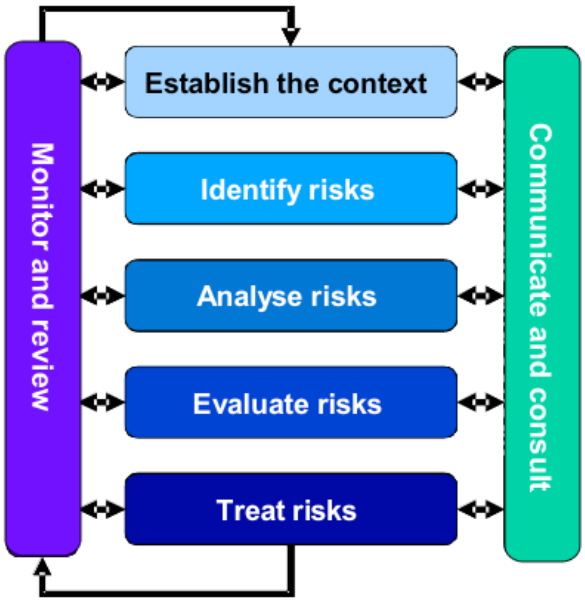
The results of the Customer Satisfaction surveys concerning timeliness, positive outcomes, and process aspects (http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback/trends-driver*) contributed to the identification of the Enterprise Business Intake and Demand Management (EBIDM) initiative.

* These links are only accessible from within the Government of Canada.

8 RISK MANAGEMENT

8.1 KEY IMPLEMENTATION RISKS AND MITIGATION PLANS

As SSC continues to standardize and transform GC's IT infrastructure, effective risk management will play an increasingly important role. Risk management tools and processes have been developed to help identify, assess, respond to, and monitor risks. Monitoring and reporting will enable the department to track key risks and implement timely mitigation strategies. The following model depicts a high level view of the risk management process that will be used to measure risks against the SMS and service improvement initiatives.



The following table identifies the risks association to the implementation of this SMS:

Risk #	Risk Identification	Risk Response
1	**Partnership Management:** Lack of communication and engagement with customers and SSC employees is likely to cause frustration and delays in the implementation of the service improvement intiatives.	• Engage Corporate Communications to establish a communication strategy and plan for both internal and external audiences; • Bilateral customer engagement, including departmental executive committees of customer organizations, CIO forums, steering and advisory committees; and • Ensure that the regular status reports on the implementation of the service improvement initiatives are communicated to all stakeholders.
2	**Change Management:** **SSC:** • Employee resistance to change could negatively impact the department's ability to implement the services improvement initiatives. • Readiness of the department is crucial as the SMS will impact the way services are provisioned and delivered to our customers. **Customers:** • Customer's resistance to change could negatively impact SSC's ability to implement the services improvement initiatives. • Readiness of customers is crucial as the SMS will impact the way services are provisioned and delivered to customers.	Promote and support an innovative and agile culture throughout SSC that focuses on service excellence by: ▪ Identifying and promoting constructive behaviours; ▪ Restricting the opportunities for negative behaviour; ▪ Promoting employee engagement and open dialogue across the department through the Organizational Change Management Network and SSC Champion's Networks; ▪ Analyzing the results of the 2014 Public Service Employee Survey and aligning follow-up activities to strengthen engagement and support; ▪ Engage with the Strategic Change Office of SSC. Continuously engage customers individually and the GC business community collectively through: • Engaging with the IT integrated customer planning process; ▪ Ensuring customers engagement occurs and feedback is taken into consideration; and ▪ Engaging the Account Executives and Service Delivery Managers throughout the Service Improvement Implementation.

3	**Governance:** Clarity of SSC and customer roles and responsibilities is essential if services are to be delivered effectively and efficiently.	• Ensure clarity of roles and responsibilities between customers and SSC; • Ensure the service improvement initiative status reports are presented at the governance committees outlined in section 1.3 of this document including external advisory bodies as required.
4	**Operational Implementation:** Not implementing the SMS will prevent the department from providing customer-centric services and the quality of those services will be considerably deminished.	• Indicate through open and visible Deputy Head approval of the SMS, the full extent of internal support for the service improvement initiatives; • Apply the Project Management Centre of Excellence framework for project tracking and reporting as required; • Continue monthly publication of the Service Status Report to Senior Management; • Leverage existing service governance to drive improved service management; • Ensure that the regular status reports on the implementation of the service improvement initiatives are communicated to all stakeholders.

APPENDIX A – SERVICE MANAGEMENT STRATEGY WORK PLAN

The content below has been updated from the SMS - 2016 Annual Report.

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
Improve Service Management Approach	Provide clear information on service definition and standards. Improve organization/structure of service information to be more user-centric.	*ID01 - Static Service Inventory is updated on Serving Government Web Site.	*DG, Service Management Transformation*	Fall 2015	Green * SMS commitments 2015 -2016
		*ID02 - Implementation of an interactive portal, integrated with the Service Management Tool suite.	*DG, Service Management Transformation*	March 2018	Blue
	Identify and resolve tactical and strategic service-related issues and risks, in collaboration with the appropriate authority to drive improvements. Incorporates: Service performance metrics, Customer satisfaction and Service cost.	*ID03 - Define the approach for Service Reviews by associating operational data to the 5 priority services.	*DG, Service Management Transformation*	March 2016	Green * SMS commitments 2015 -2016
		*ID04 - Initiate and schedule Service Reviews for the 5 priority services.	*DG, Service Management Transformation*	May 2016	Green
		*ID05 – Initiate and schedule for Service Reviews for the *established* enterprise services. ***Note*** *- The word was changed to provide consistency.*	*DG, Service Management Transformation*	March 2017	Blue
	Further develop published service definition; including service ~~*standards and*~~ levels. ***Note -*** *The service standard component of this objective is now the Service Standards initiative.* * Establish Key Performance Indicators to enhance performance measurement capabilities. ***Note -*** ** This is closely tied with the recommendation from the OAG Report on a benefits management framework for services.*	*ID06 - Define a core set of service levels for the 5 priority services.	*DG, Service Management Transformation*	November 2015	Green * SMS commitments 2015 -2016
		*ID07 - Review current service levels for established enterprise services and align to core set.	*DG, Service Management Transformation*	March 2016	Green * SMS commitments 2015 -2016
		*ID08 - Ensure all new/future customer-facing services include the core set of SLEs, as Service Designs evolve.	*DG, Service Management Transformation*	March 2017	Green

*** -** Original initiative from diagram in section 1.2 Key Timeframes from the Service Management Strategy 2015 - 2018. Blue text represents changes from original Service Management Strategy 2015 - 2018.

**** -** New initiative from the Service Management Strategy 2016 Annual Report.

APPENDIX A - SERVICE MANAGEMENT STRATEGY WORKPLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
Framework of Customer Satisfaction Feedback	Improve user experience of SSC services, internal and external processes and customer engagement and relationship management practices.	*ID09 - Establish Baseline Framework. Conduct Pilot for the 43 customers.	DG, Account Teams	December 2015	Green * SMS commitments 2015 -2016
		*Explore expanding to include Business Program input. ***Note*** *- This action has been discontinued and has been replaced with ID10 to provide clarity.*	DG, Account Teams	December 2016	Grey
		*Expand to end-users / all SSC services. ***Note*** *- This action has been discontinued and has been replaced with ID13 to provide clarity.*	DG, Account Teams	December 2017	Grey
		***ID10 - Explore expanding to 132 clients (smaller departments) including a 9-client pilot.*	DG, Account Teams	December 2016	Blue
		***ID11 - Conduct an ETI service-specific customer satisfaction survey, as the priority service has completed the service authorization process and has been operational for a minimum of 6 months.*	DG, Account Teams	December 2016	Blue
		***ID12 - Expand to end-users and regional/local CIOs.*	DG, Account Teams	December 2017	Blue
		***ID13 - Identify SSC services that can have a service-specific customer satisfaction survey developed – focusing on the 5 priority services followed by the other services within the inventory.*	DG, Account Teams	December 2017	Blue

*** -** Original initiative from diagram in section 1.2 Key Timeframes from the Service Management Strategy 2015 - 2018. Blue text represents changes from original Service Management Strategy 2015 - 2018.

**** -** New initiative from the Service Management Strategy 2016 Annual Report.

APPENDIX A - SERVICE MANAGEMENT STRATEGY WORKPLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
E-enablement of SSC customer-facing services	*Streamline service provisioning by maximizing automation in the delivery of SSC services to customers where feasible.* ***Note*** *- This objective has been discontinued based on clarification received from TBS regarding Proportion of E-Services: Measurement Framework.*	*Work with the service leads to establish automation plan for the Priority Services. ***Note*** *- This action has been discontinued based on clarification received from TBS regarding Proportion of E-Services: Measurement Framework.*	*DG, Service Management Transformation*	March 2016	Grey
		*Determine level of automation for remaining customer-facing services to establish automation plans. ***Note*** *- This action has been discontinued based on clarification received from TBS regarding Proportion of E-Services: Measurement Framework.*	*DG, Service Management Transformation*	March 2017	Grey
	Streamline service provisioning by maximizing e-enablement where feasible. Improve user experience by providing on-line self-service capability.	***ID14 - Revised definitions and methodologies for the identification of service steps to be e-enabled.*	*DG, Service Management Transformation*	*August 2016*	Green
		***ID15 - Analysis of current e-enablement status for SSC customer-facing services.*	*DG, Service Management Transformation*	*September 2016*	Green
		**ID16 -* Identify which customer-facing services can be e-enabled, focus on the 5 Priority Services.	*DG, Service Management Transformation*	*September 2015*	Green * SMS commitments 2015 -2016
		***ID17 - Establish e-enablement plans for the 5 priority services.*	*DG, Service Management Transformation*	*March 2017*	Blue
		***ID18 - Establish e-enablement plans for the other services within the inventory.*	*DG, Service Management Transformation*	*March 2018*	Blue
		***ID19 - Establish mechanism(s) to enable reporting on performance and progress against targets for e-enablement of customer-facing services.*	*DG, Service Management Transformation*	*March 2017*	Blue
		***ID20 - Demonstrate progress against e-enablement plans for all services.*	*DG, Service Management Transformation*	*March 2018*	Blue
	Ensure that e-services provide a quality user experience.	**ID21 -* Establish approach for customer engagement.	*DG, Service Management Transformation*	*June 2016*	Green
		ID22 -* Engage customers to ensure their needs are incorporated within the e-services designs *and plans*. ***Note* *- This action has been updated to include the planning function.*	*DG, Service Management Transformation*	*March 2018*	Blue

*** -** Original initiative from diagram in section 1.2 Key Timeframes from the Service Management Strategy 2015 - 2018. Blue text represents changes from original Service Management Strategy 2015 - 2018.

**** -** New initiative from the Service Management Strategy 2016 Annual Report.

Legend: The status of the initiative: **Green**: Completed **Blue**: On target **Yellow**: Risk of delay **Red:** Delayed **Grey**: Discontinued

APPENDIX A - SERVICE MANAGEMENT STRATEGY WORKPLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
Service Standards	*To develop, implement and monitor Service Standards within the Department aligning to TBS Service Standards guidelines.*	*** ID23 – Refine the framework and approach for Service Standards.*	*DG, AB-TPO*	*September 2017*	Blue
		***ID24 – Develop and execute a communications plan for Service Standards.* .	*DG, AB-TPO*	*December 2017*	Blue
		***ID25 – Identify Service Standards for the 5 priority services.*	*DG, AB-TPO*	*December 2017*	Blue
		***ID26 – Identify Service Standards for the other services within the inventory.*	*DG, AB-TPO*	*December 2018*	Blue
		***ID27 – Establish a monitoring process to ensure that the use of Service Standards remains relevant to our customers.*	*DG, AB-TPO*	*December 2018*	Blue

*** -** Original initiative from diagram in section 1.2 Key Timeframes from the Service Management Strategy 2015 - 2018. Blue text represents changes from original Service Management Strategy 2015 - 2018.

**** -** New initiative from the Service Management Strategy 2016 Annual Report.

APPENDIX A - SERVICE MANAGEMENT STRATEGY WORKPLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
Enterprise Business Intake and Demand Management (EBIDM)	*A centralized enterprise approach for managing SSC demand from intake to delivery.*	*** ID28 – Develop and implement a standardized enterprise business intake process.*	*DG, Service Delivery Management*	*March 2016*	Green * SMS commitments 2015 -2016
		***ID29 – Streamline the enterprise business intake process. .*	*DG, Service Delivery Management*	*March 2017*	Blue
		***ID30 – Identify common business requests and processes that can be simplified to better meet Customer expectations.*	*DG, Service Delivery Management*	*March 2017*	Blue
		***ID31 – Develop and execute a communications plan that reinforces and emphasizes the use of the enterprise business intake process.*	*DG, Service Delivery Management*	*March 2017*	Blue

*** -** Original initiative from diagram in section 1.2 Key Timeframes from the Service Management Strategy 2015 - 2018. Blue text represents changes from original Service Management Strategy 2015 - 2018.

**** -** New initiative from the Service Management Strategy 2016 Annual Report.

APPENDIX B – SERVICE INVENTORY

The content below has been updated from the SMS - 2016 Annual Report.

Shared Services Canada (SSC) Service Inventory is provided below using the template provided by Treasury Board Secretariat.

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
0001	Email	Information Technology Services	Priority Service	Email enables individuals working for the Government of Canada to send and receive electronic mail messages and to manage a calendar, tasks, an address book and personal contacts.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Email and Mobile Enterprise Server Services	1.1.1.3	Internal	Shared Services Canada	Yes	Internal to Government	1	0	0	0	0	0	N/A	N/A	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	100%
0002	Application Hosting	Information Technology Services	Priority Service	Application Hosting provides partners with a fully managed, secure, reliable and scalable multi-tier platform, including standardized application and database middleware, which allows partners to host and manage their data and business applications. The service provides a standard approach to using these platforms in non-production (development and test), pre-production and production environments, as required by partners' systems development life cycles.	SSC - Data Centre Services Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Dedicated Application Hosting and Management Services	1.1.2.2	Internal	Shared Services Canada	Yes	Internal to Government	5	0	0	0	0	0	N/A	N/A	No	Yes	Yes	N/A	No	No	No	No	No	No	0%

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
0003	GC WAN	Information Technology Services	Priority Service	GC WAN is a fully managed network service that interconnects partner or client locations across metropolitan, regional, national or international boundaries. This service provides enterprise WAN connectivity for data centres and GC buildings and locations. It interconnects users and computers from national and international locations to each other and the Internet, while supporting business applications for simultaneous voice, data and video communications, as required.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Email and Mobile Enterprise Server Services	1.1.1.3	Internal	Shared Services Canada	Yes	Internal to Government	7	0	0	0	0	0	N/A	N/A	No	Yes	Yes	No	No	Yes	Yes	Yes	No	50%
0004	Mobile Devices	Information Technology Services	Priority Service	Mobile Device provides cellular phones, smartphones and cellular data devices, along with their service plans. Specialized solutions for emergency-response personnel and senior executives on travel status are also available.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Voice Network Services	1.1.3.3	Internal	Shared Services Canada	Yes	Internal to Government	6838	0	3	0	0	0	N/A	N/A	No	Yes	Yes	No	No	No	No	No	No	0%
0005	Videoconferencing	Information Technology Services	Priority Service	An integrated, standardized service that provides Government of Canada employees the ability to connect video enabled boardrooms and video enabled desktop endpoints between departments on the Government of Canada shared metropolitan network.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Conferencing Services	1.1.3.4	Internal	Shared Services Canada	Yes	Internal to Government	1147	0	0	0	0	0	N/A	N/A	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	67%

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
0006	Contact Centre	Information Technology Services		An integrated, standardized service that provides Government of Canada employees the ability to connect video enabled boardrooms and video enabled desktop endpoints between departments on the Government of Canada shared metropolitan network.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Conferencing Services	1.1.3.4	Internal	Shared Services Canada	Yes	Internal to Government	3	0	0	0	0	0	N/A	N/A	No	Yes	Yes	N/A	No	No	N/A	No	No	0%
0007	High-performance Computing	Information Technology Services		High Performance Computing provides a fully managed platform for extreme performance computing needs, such as intermittent computing or steady-state heavy computing in both research and production environments.	SSC - Data Centre Services Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Utility Computing Services	1.1.2.1	Internal	Shared Services Canada	Yes	Internal to Government	2	0	0	0	0	0	N/A	N/A	No	Yes	Yes	N/A	No	No	No	No	No	0%
0008	Toll-free Voice	Information Technology Services		Toll-Free Voice provides toll-free (1-800) access to Government of Canada (GC) departments and agencies across Canada.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Voice Network Services	1.1.3.3	Internal	Shared Services Canada	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	Yes	N/A	Yes	Yes	Yes	No	No	60%
0009	Fixed Line (Landline) Phones	Information Technology Services		Fixed Telephony supplies and installs telephone systems, services and devices, including: Voice over IP (VoIP), Centrex, PBX, Key systems.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Voice Network Services	1.1.3.3	Internal	Shared Services Canada	Yes	Internal to Government	3441	0	1	0	0	0	N/A	N/A	No	Yes	Yes	No	No	No	No	No	No	0%

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
0010	Software Provisioning	Information Technology Services		SSC provides and pays for workplace technology devices (WTD) software for its 43 partner organizations, which have already transferred funds earmarked for WTD software to SSC. Clients (organizations that are not one of SSC's partner departments and agencies) are also required to obtain WTD software from SSC, but will assume the costs. The Software Provisioning Service provides an end-to-end request fulfillment process for WTD software for departmental and agency IT organizations.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Desktop and Office Productivity Suite Services	1.1.1.2	Internal	Shared Services Canada	Yes	Internal to Government	1	0	0	0	0	0	N/A	N/A	No	Yes	Yes	No	No	No	No	No	No	0%
0011	File	Information Technology Services		SSC File Services for partners currently provides file share services that are centralized, scalable, online storage solutions for unstructured data. It includes root share management, quota management, data migrations, data capacity trending and reporting. SSC is also working to provide future cloud-based file solutions for partners, which will allow for offline data, and data cross-platform synchronization among devices using a new and efficient way to manage unstructured data.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	File/Print Services	1.1.1.4	Internal	Shared Services Canada	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	Yes	N/A	No	No	No	No	No	0%

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
0012	Distributed Print	Information Technology Services		Distributed Print provides industry-standard access to printing services for servers within the Government of Canada network.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	File/Print Services	1.1.1.4	Internal	Shared Services Canada	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	Yes	N/A	No	No	No	No	No	0%
0013	Bulk Print	Information Technology Services		Bulk Print provides standardized and fully managed printing to meet both high-volume and specialized print media requirements. The service offers high-volume distribution and mailing capabilities in secure, centralized printing facilities.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	File/Print Services	1.1.1.4	Internal	Shared Services Canada	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	Yes	N/A	No	No	No	No	No	0%
0014	Intra-building Network Services	Information Technology Services		Intra-Building Network Services provide Government of Canada partner and client organizations with the interconnection of network segments in building, campus, and data centre environments. These services provide a reliable means of transport for voice, data, and video based applications.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Data Network Infrastructure Services, Inter- and Intra-Data Centre Network Services	1.1.3.1, 1.1.3.2	Internal	Shared Services Canada	Yes	Internal to Government	3	0	1	0	0	0	N/A	N/A	No	Yes	Yes	No	No	N/A	N/A	No	No	0%
0015	Internet	Information Technology Services		Internet (Local Access) provides connectivity for GCNet users to access the Internet and for the public to access Government of Canada websites.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Data Network Infrastructure Services	1.1.3.1	Internal	Shared Services Canada	Yes	Internal to Government	157	0	1	0	0	0	N/A	N/A	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	67%

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
0016	Satellite	Information Technology Services		Satellite provides satellite-based telecommunications infrastructure. The offering includes fixed and mobile solutions, as well as national and international options.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Data Network Infrastructure Services	1.1.3.1	Internal	Shared Services Canada	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	No	50%
0017	Teleconferencing (Audio conferencing)	Information Technology Services		Audio Conferencing allows multiple participants to collaborate by telephone anytime, anywhere, with or without operator assistance.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Voice Network Services	1.1.3.3	Internal	Shared Services Canada	Yes	Internal to Government	33	0	0	0	0	0	N/A	N/A	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	100%
0018	Web Conferencing	Information Technology Services		Web conferencing allows users to conduct a conference over the Web. Content from the screen of the meeting host, or from a participant's computer, is displayed on all participants' computers. This includes documents, applications, browsing sessions and live desktop video.	SSC - Network and End Users Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Conferencing Services	1.1.3.4	Internal	Shared Services Canada	Yes	Internal to Government	14	0	0	0	0	0	N/A	N/A	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	100%

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
0019	myKEY	Information Technology Services		myKEY is an internal credential management (ICM) service that facilitates authentication for secure access to applications and Government of Canada networks. It is used to eliminate potential deniability of transactions using digital signatures and to facilitate the exchange of encrypted email and documents for Protected B information. It is also used for authentication between users, applications and devices (e.g. Compensation Web Applications (CWA) and Government of Canada Secure Remote Access (GCSRA)).	SSC - Cyber and IT Security Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Identification, Authentication and Authorization Services	1.1.4.2	Internal	Shared Services Canada	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	Yes	Yes	N/A	N/A	No	Yes	Yes	75%
0020	External Credential Management	Information Technology Services		Cyber Authentication is an external credential management (ECM) service provided by the Government of Canada to allow the public and businesses to securely conduct online business with various governmental programs and services. Use of this service is mandatory for Government of Canada departments and agencies.	SSC - Cyber and IT Security Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Identification, Authentication and Authorization Services	1.1.4.2	Internal	Shared Services Canada	Yes	Internal to Government	406	0	0	0	0	0	N/A	N/A	No	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	100%

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
0021	Secure Remote Access	Information Technology Services		Government of Canada Secured Remote Access (GCSRA) provides users with the ability to securely transmit and receive information from remote client workstations or remote gateways while maintaining the availability, confidentiality and integrity of the data.	SSC - Cyber and IT Security Branch	Shared Services Canada Act (S.C. 2012, c. 19, s. 711)	Remote Access Services, Identification, Authentication and Authorization Services, Secure Communication Services	1.1.1.5, 1.1.4.2, 1.1.4.3	Internal	Shared Services Canada	Yes	Internal to Government	3	0	0	0	0	0	N/A	N/A	No	Yes	Yes	N/A	No	No	No	No	No	0%
022	Microcomputers	Information Technology Services		SSC mandated goods and services for purchase against existing procurement vehicles using a web-hosted electronic store (e-store) called SSC IT Pro. This ordering portal is only to be used by government employees who have the authority from their organization to order the goods and services available on the portal (procurement authorities and certain IT groups).	SSC - Procurement and Vendor Relationships	Shared Services Canada Act (Order In Council 2015-1071)	Workstation Services	1.1.1.1	Internal	Shared Services Canada	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	100%
023	Networking Equipment	Information Technology Services		The Networking Equipment service provides access to Network Equipment Support Services (NESS) standing offers (SOs) for the supply, delivery and optional configuration and installation of purchased networking equipment, with associated warranty services, and Network Infrastructure Management Services (NIMS) standing offers (SOs) to procure maintenance services for network hardware, software and licenses.	SSC - Procurement and Vendor Relationships	Shared Services Canada Act (Order In Council 2015-1071)	Data Network Infrastructure Services, Inter- and Intra-Data Centre Network Services, Voice Network Services	1.1.3.1, 1.1.3.2, 1.1.3.3	Internal	Shared Services Canada	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	No	Yes	Yes	Yes	No	Yes	No	67%

Service ID Number	Service Name	Service Type	Special Designations	Service Description	Responsibility Area	Authority	Program Name	Program ID Number	External Service or Internal Enterprise Service	Service Owner	Service Agreements	Clients/Service Target Groups	Volumes per Channel (Applications (A) and Outputs (O))								User Fee	Service Standards	Operational Performance Targets	E-Enabled Services						
													Online		Telephone		In Person		Mail					Account Registration/ Enrollment	Authentication	Application	Decision	Issuance	Issue Resolution and Feedback	Estimated % of the service completed online
													A	O	A	O	A	O	A	O										
024	Printing Products	Information Technology Services		The Printing Products service provides access to document scanner standing offer (SO) for the supply, delivery, installation and service of document scanners, including accessories and supplies on an "as and when requested" basis to locations throughout Canada, excluding comprehensive land claims areas, and Imaging hardware standing offer (SO) to enable Government of Canada departments and agencies to purchase or lease a variety of connected and unconnected digital copying and printing equipment, both monochrome and colour.	SSC - Procurement and Vendor Relationships	Shared Services Canada Act (Order In Council 2015-1071)	Desktop and Office Productivity Suite Services, File/Print Services	1.1.1.2, 1.1.1.4	Internal	Yes	Yes	Internal to Government	0	0	0	0	0	0	N/A	N/A	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	83%

APPENDIX C – DOCUMENT REFERENCES

The following is a list of all documents referenced or referred to in SSC Service Management Strategy 2015 - 2018 document.

Ref. No.	Document Name, Version	Brief Description	Location of Definitive Source
Ref 1	SSC Integrated Business Plan 2014-15		Link/location
Ref 2	TBS Policy on Service	Objective, expected results and principles.	*http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27916
Ref 3	MAF 2014-15 Departmental Report	Objective	
Ref 3	2015–16 Report on Plans and Priorities	Services	*http://ssc-spc.gc.ca/pages/rpp2015-2016-eng.html#s1a
Ref 4	Guideline on Service Standards		*http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25750
Ref 5	SSC Directive on Performance Measurement	Performance Framework	Document
Ref 6	Integrated Risk Management Framework	Risk Framework	
Ref 7	Risk Management Guide	Guide to Risk Management Process	
Ref 8	Departmental Performance Report 2013-14	Actual Performance Results	*http://ssc-spc.gc.ca/pages/dpr2013-14-rmr-eng.html
Ref 9	Departmental Audit and Evaluation Committee	Purpose, Objectives	*http://www.ssc-spc.gc.ca/pages/gvrnnc-daec-cmve-eng.html
Ref 10	SSC Integrated Business Plan 2015-16	Priorities	Document
Ref 11	Governance Committees	Governance	*http://www.ssc-spc.gc.ca/pages/gvrnnc-eng.html
Ref 12	ITIR	Priorities	*http://ssc-spc.gc.ca/pages/itir-triti/itir-may2615-pres1-eng.html
Ref 13	Departmental Audit and Evaluation Committee	Mandate	*http://www.ssc-spc.gc.ca/pages/gvrnnc-daec-cmve-eng.html
Ref 14	Workplace 2.0	Objectives	*http://www.tpsgc-pwgsc.gc.ca/biens-property/mt-wp/faq-eng.html
Ref 15	Open Government	Objectives	*http://open.canada.ca/en/content/canadas-action-plan-open-government-2014-16

* These links are only accessible from within the Government of Canada.

The content below has been updated from the SMS - 2016 Annual Report.

The following is a list of all documents referenced or referred to in SSC Service Management Strategy - 2016 Annual Report document.

Ref. No.	Document Name, Version	Brief Description	Location of Definitive Source
Ref 1	SSC Integrated Business Plan 2015–16	IBP describes SSC's mandate, context and priorities and highlights specific activities we will undertake to achieve these priorities.	*http://www.ssc-spc.gc.ca/pages/ibp-pai-2015-2016-eng.html
Ref 2	TBS Policy on Service	Objective, expected results and principles.	*http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27916
Ref 3	MAF 2015–16 Departmental Report	Progress related to government-wide priorities and the state of policy transformation.	Document
Ref 4	2016–17 Report on Plans and Priorities	SSC provides information on how the department will support the Government on achieving our agenda in the coming year.	*http://www.ssc-spc.gc.ca/pages/rpp2016-2017-eng.html
Ref 5	Guideline on Service Standards	The Guideline on Service Standards provides general guidance on the use of service standards across the Government of Canada.	*http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25750
Ref 6	2015 Fall Reports of the Auditor General of Canada	Performance audit conducted by the Office of the Auditor General of Canada under the authority of the *Auditor General Act*.	*http://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_04_e_41061.html
Ref 7	Budget 2016	Budget 2016 reflects the new approach to supporting Canadians.	*http://www.budget.gc.ca/2016/docs/plan/budget2016-en.pdf
Ref 8	Government of Canada – Information Technology Strategic Plan 2016–2020	Four-year strategic direction for Information Technology (IT) in the federal government.	*http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/itpm-itgp/it-ti/itsp-tips-eng.asp?utm_source=referral&utm_medium=news&utm_term=canada&utm_content=landing&utm_campaign=itstrat
Ref 9	House of Commons: Report 4, Information Technology Shared Services (of the 2015 OAG Report)	House of Commons committee study on Chapter 4, Information Technology Shared Services, of the Fall 2015 Report of the Auditor General of Canada.	*http://www.parl.gc.ca/Content/HOC/Committee/421/PACP/Reports/RP8305326/421_PACP_Rpt09_PDF/421_PACP_Rpt09-e.pdf
Ref 10	SSC Integrated Business Plan 2016–17	IBP describes SSC's mandate, context and priorities and highlights specific activities we will undertake to achieve these priorities.	*http://myssc-monspc.ssc-spc.gc.ca/en/our-organization/priorities/ibp/2016-17

* These links are only accessible from within the Government of Canada.

Service | Innovation | Value

SHARED SERVICES CANADA

Service Management Strategy (SMS) 2015–2018

2016 Annual Report

Version: Final

Date: October 17, 2016

Doc ID: TBD

APPROVAL

Shared Services Canada's Service Management Strategy – 2016 Annual Report

The signing authority below concurs with the content of this document.

Executive Sponsor: Shared Services Canada's Deputy Head

Name:	Ron Parker, President		
Signature:	Ron Parker	Date:	NOV 0 2 2016

Shared Services Canada's Service Management Strategy – 2016 Annual Report received formal approval from the Senior Management Board on October 12, 2016.

TABLE OF CONTENTS

Annual Report Context

The Policy on Service requires that “a multi-year departmental service management strategy be developed every three (3) years and implemented in alignment with the Government of Canada (GC) service direction, and that progress be measured annually.”

This Shared Services Canada (SSC) Service Management Strategy (SMS) 2016 Annual Report details changes made to our approved SSC 2015–2018 Service Management Strategy found at http://service.ssc-spc.gc.ca/en/policies_processes/service-manage-strategy-report and progress made on the SMS Work Plan.

All changes to the Service Management Strategy have been highlighted in *blue italics* in the sections below.

1 INTRODUCTION

1.1 PURPOSE

No changes have been made to this section. Refer to Appendix A for details regarding initiatives and activities.

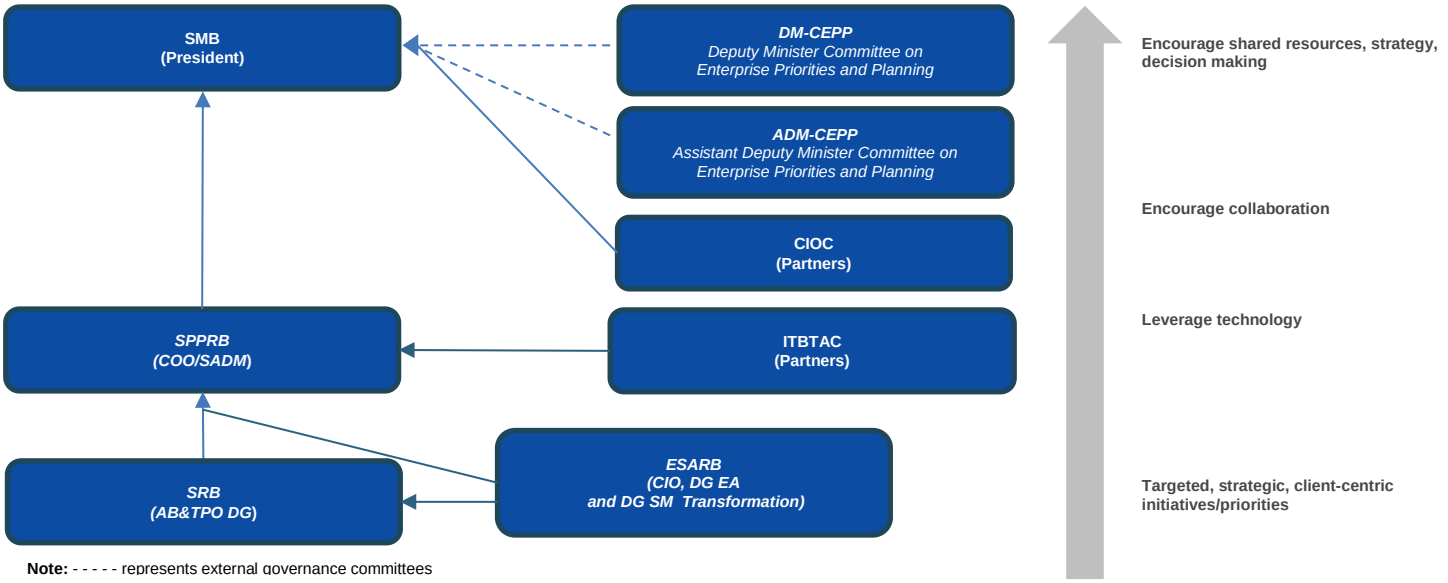
1.2 KEY TIMEFRAMES

The three-year period covered by the Service Management Strategy remains 2015–2018. Refer to Appendix A for details regarding initiatives and activities.

1.3 GOVERNANCE

The Government of Canada IT Strategic Plan 2016-2020 includes two new government wide governance committees - The Deputy Minister and Assistant Deputy Minister Committees on Enterprise Priorities and Planning (CEPP) will be the governance and oversight bodies for all government IT investments. These external committees are now included in the diagram below and will manage demand from departments and agencies for SSC IT infrastructure services, and guide how SSC provides those supply-side services.
In addition, there have been three changes to our internal governance committees to improve our customer-centric approach to enterprise services and demonstrate operational efficiencies to our customers.

Updated content



Note: - - - - - represents external governance committees

Senior Management Board (SMB)
Chair, President

- Senior Management Board (SMB) is SSC's Senior Executive decision-making forum – full decision-making authority;
- Strategic direction, priority setting and broad oversight (i.e., "steering role");
- Sets strategic direction and enterprise-wide priorities;
- Approves corporate-wide plans, strategies, and monitoring and reporting requirements.

Service, Project and Procurement Review Board (SPPRB)
Chair, COO

- *The Service, Project and Procurement Review Board's (SPPRB) key role is to provide guidance and oversight to senior management with respect to all service lines and projects, ensuring alignment with SSC's strategic and service objectives.*
- *The SPPRB serves as the first level of escalation for systemic service-delivery issues before referral to the Senior Management Board (SMB). Proactive efforts should be made to discuss unresolved service-delivery issues at the SPPRB before partners or clients submit formal complaints at the Deputy Minister level.*

Service Review Board (SRB)
Chair, AB&TPO DG

- *As a Director General (DG) sub-committee of the Service, Project and Procurement Review Board (SPPRB), the Service Review Board (SRB) has the key role of overseeing the management of Shared Services Canada's (SSC) enterprise services throughout their life cycle, including service authorization and the management of associated risk. More specifically, the SRB ensures that all elements of the service portfolio management framework that are necessary for successful service transformation are in place horizontally across the organization and are being adhered to.*

Enterprise Strategies and Architecture Review Board (ESARB)
Co-Chairs, CIO, DG EA and DG SM Transformation

- *The Enterprise Strategy and Architecture Review Board's (ESARB) key role is to provide advice to senior management with respect to the evolution of enterprise strategies and associated architectures, ensuring that they are aligned with Shared Services Canada's (SSC) mandate and authority and support the Government of Canada's priorities. This role includes providing SSC and its partners and clients with guidance and oversight with respect to the future vision of SSC's offerings.*

DM-CEPP
Deputy Minister Committee on
Enterprise Priorities and Planning

The coordinating body for enterprise and common services to ensure the consideration of business and enterprise priorities and guide the implementation of the Government of Canada IT Strategic Plan (strategic plan) to improve service delivery for clients and Canadians.
Responsibilities

- *As the coordinating body for enterprise and common services, DM CEPP will:*
- *Recommend enterprise and common approaches for the delivery of which government services should be adopted*
- *Support and enable departments and agencies to adopt enterprise solutions for consolidated services, and recommend the pace at which departments and agencies adopt enterprise IT solutions*
- *Guide the balance of supply and demand, and ensure investments are sustainable and add business value*
- *Consider recommendations on priorities and projects from the subordinate ADM-level committee(s) (i.e. ADM-CEPP)*

ADM-CEPP
Assistant Deputy Minister Committee on Enterprise Priorities and Planning

The ADM Committee on Enterprise Priorities and Planning will support the PSMAC Sub-Committee on Enterprise Priorities and Planning by:

- *Advising on the development and implementation of a GC-wide IT strategy and policies that reflect business and enterprise-wide priorities and that enable improved service delivery to clients and Canadians;*
- *Assessing the aggregate risk of the GC's IT portfolio and reviewing risk mitigation strategies;*
- *Developing a principles-based framework for prioritizing IT projects and balancing capacity and demand that reflects enterprise needs;*
- *Applying the principles-based framework as approved by the PSMAC Sub-Committee on Enterprise Priorities and Planning to make recommendations on projects that should proceed and to identify interdependencies and opportunities for integration;*
- *Reviewing the development, implementation and updating of a GC Integrated IT Plan;*
- *Proactively anticipating and resolving prioritization conflicts between major competing initiatives and determining appropriate trade-offs when required; and,*
- *Providing reports and recommendations to the PSMAC Sub-Committee on Enterprise Priorities and Planning on any of the above issues.*

Chief Information Officer Council (CIOC)
Chair, Departmental senior officials

- The Chief Information Officer Council is a forum for consultation and information exchange on matters relating to the effective management and use of information and technology in support of program and service delivery in the Government of Canada. The Chief Information Officer (CIO) Council is made up of departmental senior officials responsible for Information Management and Information Technology in their departments.

Information Technology Business Transformation Advisory Committee (ITBTAC)
Chair, Strategy Branch SADM

- IT Business Transformation Advisory committee provides advice to SSC on issues related to the delivery of ongoing IT services;
- Ways to improve quality, timeliness and responsiveness of services, continuous improvement;
- Approaches to enhance client satisfaction and engagement.

2 SSC Departmental Context

2.1 SSC's Operational Context

No changes have been made to this section.

2.2 Department's Mandate and Key Responsibilities Related to Service

No changes have been made to this section.

2.3 Services Covered by the Service Management Strategy

The section has been updated to provide clarity regarding which services are being addressed within this three (3)-year Service Management Strategy as a result of feedback received in The Fall 2015 Report from the Office of the Auditor General (OAG). The annual service review cycle has begun with the focus on the 5 priority services. The Videoconferencing service review has been completed and the remaining priority service reviews will be completed by spring 2017. Results of these services reviews will be included in the SSC SMS - 2017 Annual Report.

Updated content

SSC's pursuit to improve the department's SMS is integral to meeting customer-centric, efficiency and service excellence goals. Each year, SSC will update and implement the list of service improvement initiatives to incrementally realize the three-year SMS objective. *Service improvements outlined in Appendix A are for all SSC services and are defined in the context of both legacy and enterprise environments.*

2.4 Relationship to Other Departmental or GC-wide Investments or Initiatives

No changes have been made to this section.

3 DEPARTMENTAL SERVICE VISION

Departmental service vision has been updated to reflect that the SMS covers all services based on recommendations from The Fall 2015 Report from the Office of the Auditor General (OAG).

Updated content

SSC's vision *is to provide modern, reliable, secure and cost-effective IT infrastructure services to support government priorities and program delivery*.

SSC is committed to meeting the needs of its customers through improving its service management approach; *SSC's vision for service applies to all services, including legacy and enterprise services. Budget 2016 included additional funding for SSC to maintain legacy equipment as the transition to enterprise services is ongoing. An ongoing evergreening strategy for all services is being developed as part of SSC's Transformation Plan reset in fall 2016.*

The SMS reflects SSC's overall vision to

- → provide customer-centric, cost-effective shared services that improve service delivery;
- → improve the customer experience, increase efficiencies, and reduce delivery costs; and
- → provide best value to customers.

SSC is dedicated to demonstrating results and realizing cost efficiencies through the transformation of Government of Canada IT infrastructure services. We have taken a collaborative approach by engaging customers to participate in a delivery-cost-reduction exercise to reduce the overall costs of SSC services.

To achieve the service vision, SSC must be in constant engagement with its stakeholders for the planning, design and delivery of SSC's service inventory. *The service improvement initiatives outlined in Appendix A demonstrates the department's commitment* to ensuring that the priorities are at the forefront of how SSC will meet its vision and objectives. A critical enabler of supporting how SSC addresses the priorities will be to leverage existing and emerging service trends.

4 DEPARTMENTAL SWOT ANALYSIS

The SWOT analysis has been updated to take into consideration the recommendation from The Fall 2015 Report from the Office of the Auditor General (OAG) and the results of the Customer Satisfaction Surveys http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback/monthly-results concerning timeliness, positive outcomes and process aspects.

Updated content

Strengths	Weaknesses	Opportunities	Threats
An organization's strengths are its resources and capabilities that can be used for developing competitive advantage.	The absence of certain strengths may be viewed as weaknesses or, in this case, the gap between what SSC aspires to be and its current level of service management process and organizational maturity.	The external environmental analysis may reveal new opportunities for excellence or growth.	Changes in the external environment may also present threats to the organization.
1.0) Strong support for Service Management evolution and improvement from President, COO and Executive Leadership Team.*	1.0) Service Management evolution and improvement plans are evolving, have not been fully communicated and/or are not fully accepted across the Department.*	1.0) Implement the SMS and ensure that the service improvement plans are widely communicated and understood across the organization.* 1.1) Leverage the GC IT prioritization committees to ensure alignment.*	*1.0) Departmental service priorities could be impacted by potential legislative and/or other GC priorities.**
**Note: Strength, Weakness, Opportunity and Threat analysis 1.0 has been addressed as follows:* *SSC's SMS has been communicated across the organization through official communications as well as published on the My SSC portal. Service improvement plans have been communicated and are understood across the organization. All actions for this opportunity have been completed.*			
2.0) Recent reorganization (April 1, 2015) of SSC around lines of service enables a more service- and customer-centric approach to the delivery of services.*	2.0) Customer expectations are not well understood by the lines of service.*	2.0) Develop service levels that will satisfy customer expectations within acceptable costs to GC.*	2.0) Lack of appropriate customer participation.*
**Note: Strength, Weakness, Opportunity and Threat analysis 2.0 has been addressed as follows:* *Service levels have been completed and are posted on the SSC Service Catalogue, which is available on both the My SSC and Serving Government portals. All actions for this opportunity have been completed.*			
3.0) Strong understanding of technology within the lines of service.*	3.0) End-to-end Service Management is not fully understood within the lines of service. Focus is primarily on technical components.*	3.0) Establish a service review that will provide a holistic review of service performance from a customer request through to SSC fulfilment.*	3.0) A mismatch between the customer's view of service quality and SSC's view.*
Note: Strength, Weakness, Opportunity and Threat analysis 3.0 has been addressed as follows: *A formal service review process has been developed and approved. All SSC services are scheduled for formal review at least once during the period covered by the strategy. All actions for this opportunity have been completed.*			

4.0) Service inventory, established ownership, accountability and responsibility for each service is assigned.	4.0) Service Information within the SSC service portal is largely IT-focused and is not presented in customer service business terms.	4.0) Enhance SSC's single-service portal by providing appropriate service information and ensuring a quality e-enabled experience for customers.	4.0) Inability to satisfy customer needs.
5.0) Formal customer engagement is established at the COO and Executive Leadership Team levels through the IT Service Management Advisory Committee (ITSMAC), the **IT Business Transformation Advisory Committee (**ITBTAC) and the Chief Information Officer Council (CIOC).*	5.0) A formal mechanism to monitor and measure customer feedback on the performance and management of the services has not been implemented.*	5.0) Establish a formal customer satisfaction mechanism in order to monitor and measure the performance and management of services and identify areas for improvement.*	5.0) Lack of appropriate customer participation.*

**Note: Strength, Weakness, Opportunity and Threat analysis 5.0 has been addressed as follows:*
A formal customer satisfaction mechanism has been developed and approved. The results are available on the SSC Serving Government portal located at http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback. All actions for this opportunity have been completed.

6.0) Recent reorganization (August 18, 2016) of SSC's Service Delivery and Management organization has increased leadership capacity to focus on customer-centric service delivery and Enterprise Business Intake and Demand Management (EBIDM).	*6.0) Multiple channels of customer business intake are still possible.*	*6.0) Mature the enterprise business intake and demand management processes, allowing for better management of demand and service delivery in support of customer needs and expectations.*	*6.0) Lack of appropriate customer participation.*
7.0) Service Level Expectations are defined for all SSC Services and are included within the Service Catalogue.	*7.0) Service Standards guidelines are not fully understood.*	*7.0) Refine the framework and approach aligning to TBS Service Standards guidelines.*	*7.0) Departmental service priorities could be impacted by potential legislative and/or other GC priorities.**

5 SERVICE IMPROVEMENT OBJECTIVES AND INITIATIVES

5.1 SERVICE IMPROVEMENT OBJECTIVES

No changes have been made to this section.

5.2 SERVICE IMPROVEMENT INITIATIVES

Over the past year, significant progress has been made, and in some cases activities have been completed ahead of schedule, allowing for new initiatives to be identified.

Existing Initiatives

For updates on existing initiatives, refer to Appendix A.

New Initiatives

Updated content

E-enablement

In alignment with the Policy on Service requirement 7.9 effective October 1, 2016, the Department must ensure that the proportions of internal enterprise services are e-enabled and that clear targets for increasing the proportion of e-services are established. To this end, the e-enablement of services is now a separate initiative to ensure proper focus and monitoring of this key policy requirement. The initiative identifies key deliverables that must be put in place prior to the establishment of the targets in 2016–2017. For further details on this service improvement initiative, refer to Appendix A.

Service Standards

The MAF 2015–2016 Departmental Report identified the need to further refine the overall approach to service performance reporting, including increasing the comprehensiveness and the consistency of, and improving client access to, service standards and related performance information. To this end, the initiative will refine the framework and approach to Service Standards and performance reporting, ensuring alignment with the Treasury Board Secretariat guideline on Service Standards, in accordance with the Policy on Service. For further details on this service improvement initiative, refer to Appendix A.

Enterprise Business Intake and Demand Management (EBIDM)

The Customer Satisfaction Feedback Initiative (CSFI) has issued surveys to chief information officers (CIOs) in our customer organizations since December 2015, and the results of the surveys can be found at http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback. The Enterprise Business Intake and Demand Management (EBIDM) initiative was created as a result of the feedback concerning timeliness, positive outcomes, and process aspects (http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback/trends-driver) received from the surveys. This initiative will provide a centralized enterprise approach to managing SSC demand from intake to delivery. For further details on this service improvement initiative, refer to Appendix A.

6 COMMUNICATIONS AND ENGAGEMENT

No changes have been made to this section.

7 PERFORMANCE FRAMEWORK

A new sub-section 7.3 has been included as per Treasury Board Secretariat guidance.

7.1 PERFORMANCE MEASUREMENT PLAN

No changes have been made to this section.

7.2 EVALUATION APPROACH

No changes have been made to this section.

7.3 *PERFORMANCE MONITORING, REPORTING AND RECALIBRATION*

In 2016, we monitored service performance by means of ongoing monthly operational performance reviews (OPR) by the senior management committee, the quarterly release of an IT systems health report for partners (http://service.ssc-spc.gc.ca/en/aboutus/partners/partwork/it-health/rep2) and monthly and annual customer satisfaction surveys.

The results of the Customer Satisfaction surveys concerning timeliness, positive outcomes, and process aspects (http://service.ssc-spc.gc.ca/en/aboutus/customer-satisfaction-feedback/trends-driver) contributed to the identification of the Enterprise Business Intake and Demand Management (EBIDM) initiative.

8 RISK MANAGEMENT

8.1 KEY IMPLEMENTATION RISKS AND MITIGATION PLANS

No changes have been made to this section.

APPENDIX A – SERVICE MANAGEMENT STRATEGY WORK PLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
Improve Service Management Approach	Provide clear information on service definition and standards. Improve organization/structure of service information to be more user-centric.	ID01 - Static Service Inventory is updated on Serving Government Web Site.	*DG, Service Management Transformation*	Fall 2015	Green * SMS commitments 2015 -2016
		ID02 - Implementation of an interactive portal, integrated with the Service Management Tool suite.	*DG, Service Management Transformation*	March 2018	Blue
	Identify and resolve tactical and strategic service-related issues and risks, in collaboration with the appropriate authority to drive improvements. Incorporates: Service performance metrics, Customer satisfaction and Service cost.	ID03 - Define the approach for Service Reviews by associating operational data to the 5 priority services.	*DG, Service Management Transformation*	March 2016	Green * SMS commitments 2015 -2016
		ID04 - Initiate and schedule Service Reviews for the 5 priority services.	*DG, Service Management Transformation*	May 2016	Green
		ID05 – Initiate and schedule for Service Reviews for the *established* enterprise services. ***Note*** *- The word was changed to provide consistency.*	*DG, Service Management Transformation*	March 2017	Blue
	Further develop published service definition; including service ~~*standards and*~~ levels. ***Note -*** *The service standard component of this objective is now the Service Standards initiative.* * Establish Key Performance Indicators to enhance performance measurement capabilities. ***Note -*** ** This is closely tied with the recommendation from the OAG Report on a benefits management framework for services.*	ID06 - Define a core set of service levels for the 5 priority services.	*DG, Service Management Transformation*	November 2015	Green * SMS commitments 2015 -2016
		ID07 - Review current service levels for established enterprise services and align to core set.	*DG, Service Management Transformation*	March 2016	Green * SMS commitments 2015 -2016
		ID08 - Ensure all new/future customer-facing services include the core set of SLEs, as Service Designs evolve.	*DG, Service Management Transformation*	March 2017	Green

Legend: The status of the initiative: **Green**: Completed **Blue**: On target **Yellow**: Risk of delay **Red:** Delayed **Grey**: Discontinued

APPENDIX A – SERVICE MANAGEMENT STRATEGY WORK PLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
Framework of Customer Satisfaction Feedback	Improve user experience of SSC services, internal and external processes and customer engagement and relationship management practices.	ID09 - Establish Baseline Framework. Conduct Pilot for the 43 customers.	DG, Account Teams	December 2015	Green * SMS commitments 2015 -2016
		Explore expanding to include Business Program input ***Note*** *- This action has been discontinued and has been replaced with ID10 to provide clarity.*	DG, Account Teams	December 2016	Grey
		Expand to end-users / all SSC services ***Note*** *- This action has been discontinued and has been replaced with ID13 to provide clarity.*	DG, Account Teams	December 2017	Grey
		ID10 - Explore expanding to 132 clients (smaller departments) including a 9-client pilot	DG, Account Teams	December 2016	Blue
		ID11 - Conduct an ETI service-specific customer satisfaction survey, as the priority service has completed the service authorization process and has been operational for a minimum of 6 months.	DG, Account Teams	December 2016	Blue
		ID12 - Expand to end-users and regional/local CIOs.	DG, Account Teams	December 2017	Blue
		ID13 - Identify SSC services that can have a service-specific customer satisfaction survey developed – focusing on the 5 priority services followed by the other services within the inventory.	DG, Account Teams	December 2017	Blue

Legend: The status of the initiative: **Green**: Completed **Blue**: On target **Yellow**: Risk of delay **Red:** Delayed **Grey**: Discontinued

APPENDIX A – SERVICE MANAGEMENT STRATEGY WORK PLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
E-enablement of SSC customer-facing services	*Streamline service provisioning by maximizing automation in the delivery of SSC services to customers where feasible.* ***Note*** *- This objective has been discontinued based on clarification received from TBS regarding Proportion of E-Services: Measurement Framework.*	*Work with the service leads to establish automation plan for the Priority Services;* ***Note*** *- This action has been discontinued based on clarification received from TBS regarding Proportion of E-Services: Measurement Framework.*	*DG, Service Management Transformation*	March 2016	Grey
		Determine level of automation for remaining customer-facing services to establish automation plans. ***Note*** *- This action has been discontinued based on clarification received from TBS regarding Proportion of E-Services: Measurement Framework.*	*DG, Service Management Transformation*	March 2017	Grey
	Streamline service provisioning by maximizing e-enablement where feasible. Improve user experience by providing on-line self-service capability.	*ID14 - Revised definitions and methodologies for the identification of service steps to be e-enabled.*	*DG, Service Management Transformation*	*August 2016*	Green
		ID15 - Analysis of current e-enablement status for SSC customer-facing services.	*DG, Service Management Transformation*	*September 2016*	Green
		ID16 - Identify which customer-facing services can be e-enabled, focus on the 5 Priority Services.	*DG, Service Management Transformation*	*September 2015*	Green * SMS commitments 2015 -2016
		ID17 - Establish e-enablement plans for the 5 priority services.	*DG, Service Management Transformation*	*March 2017*	Blue
		ID18 - Establish e-enablement plans for the other services within the inventory.	*DG, Service Management Transformation*	*March 2018*	Blue
		ID19 - Establish mechanism(s) to enable reporting on performance and progress against targets for e-enablement of customer-facing services.	*DG, Service Management Transformation*	*March 2017*	Blue
		ID20 - Demonstrate progress against e-enablement plans for all services.	*DG, Service Management Transformation*	*March 2018*	Blue
	Ensure that e-services provide a quality user experience.	*ID21 -* Establish approach for customer engagement.	*DG, Service Management Transformation*	*June 2016*	Green
		ID22 - Engage customers to ensure their needs are incorporated within the e-services designs *and plans*. ***Note*** *- This action has been updated to include the planning function.*	*DG, Service Management Transformation*	*March 2018*	Blue

Legend: The status of the initiative: **Green**: Completed **Blue**: On target **Yellow**: Risk of delay **Red:** Delayed **Grey**: Discontinued

APPENDIX A – SERVICE MANAGEMENT STRATEGY WORK PLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
Service Standards	*To develop, implement and monitor Service Standards within the Department aligning to TBS Service Standards guidelines.*	*ID23 – Refine the framework and approach for Service Standards.*	*DG, AB-TPO*	*September 2017*	Blue
		ID24 – Develop and execute a communications plan for Service Standards. .	*DG, AB-TPO*	*December 2017*	Blue
		ID25 – Identify Service Standards for the 5 priority services.	*DG, AB-TPO*	*December 2017*	Blue
		ID26 – Identify Service Standards for the other services within the inventory.	*DG, AB-TPO*	*December 2018*	Blue
		ID27 – Establish a monitoring process to ensure that the use of Service Standards remains relevant to our customers.	*DG, AB-TPO*	*December 2018*	Blue

Legend: The status of the initiative: **Green**: Completed **Blue**: On target **Yellow**: Risk of delay **Red:** Delayed **Grey**: Discontinued

APPENDIX A – SERVICE MANAGEMENT STRATEGY WORK PLAN

Name of the Initiative	Objectives	Actions	Area Responsible for the Initiative	Expected Completion Date	Status
Enterprise Business Intake and Demand Management (EBIDM)	*A centralized enterprise approach for managing SSC demand from intake to delivery.*	*ID28 – Develop and implement a standardized enterprise business intake process.*	*DG, Service Delivery Management*	*March 2016*	Green * SMS commitments 2015 -2016
		ID29 – Streamline the enterprise business intake process. .	*DG, Service Delivery Management*	*March 2017*	Blue
		ID30 – Identify common business requests and processes that can be simplified to better meet Customer expectations.	*DG, Service Delivery Management*	*March 2017*	Blue
		D31 – Develop and execute a communications plan that reinforces and emphasizes the use of the enterprise business intake process.	*DG, Service Delivery Management*	*March 2017*	Blue

Legend: The status of the initiative: **Green**: Completed **Blue**: On target **Yellow**: Risk of delay **Red:** Delayed **Grey**: Discontinued

APPENDIX B – SERVICE INVENTORY

Shared Services Canada (SSC) Service Inventory is a separate document using the template provided by Treasury Board Secretariat.

APPENDIX C – DOCUMENT REFERENCES

The following is a list of all documents reviewed to formulate this SMS 2016 annual update.

Ref. No.	Document Name, Version	Brief Description	Location of Definitive Source
Ref 1	SSC Integrated Business Plan 2015–16	IBP describes SSC's mandate, context and priorities and highlights specific activities we will undertake to achieve these priorities.	http://www.ssc-spc.gc.ca/pages/ibp-pai-2015-2016-eng.html
Ref 2	TBS Policy on Service	Objective, expected results and principles.	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27916
Ref 3	MAF 2015–16 Departmental Report	Progress related to government-wide priorities and the state of policy transformation.	Document
Ref 4	2016–17 Report on Plans and Priorities	SSC provides information on how the department will support the Government on achieving our agenda in the coming year.	http://www.ssc-spc.gc.ca/pages/rpp2016-2017-eng.html
Ref 5	Guideline on Service Standards	The Guideline on Service Standards provides general guidance on the use of service standards across the Government of Canada.	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25750
Ref 6	2015 Fall Reports of the Auditor General of Canada	Performance audit conducted by the Office of the Auditor General of Canada under the authority of the *Auditor General Act*.	http://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_04_e_41061.html
Ref 7	Budget 2016	Budget 2016 reflects the new approach to supporting Canadians.	http://www.budget.gc.ca/2016/docs/plan/budget2016-en.pdf
Ref 8	Government of Canada – Information Technology Strategic Plan 2016–2020	Four-year strategic direction for Information Technology (IT) in the federal government.	http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/itpm-itgp/it-ti/itsp-tips-eng.asp?utm_source=referral&utm_medium=news&utm_term=canada&utm_content=landing&utm_campaign=itstrat
Ref 9	House of Commons: Report 4, Information Technology Shared Services (of the 2015 OAG Report)	House of Commons committee study on Chapter 4, Information Technology Shared Services, of the Fall 2015 Report of the Auditor General of Canada	http://www.parl.gc.ca/Content/HOC/Committee/421/PACP/Reports/RP8305326/421_PACP_Rpt09_PDF/421_PACP_Rpt09-e.pdf
Ref 10	SSC Integrated Business Plan 2016–17	IBP describes SSC's mandate, context and priorities and highlights specific activities we will undertake to achieve these priorities.	http://myssc-monspc.ssc-spc.gc.ca/en/our-organization/priorities/ibp/2016-17

Service | Innovation | Value

SHARED SERVICES CANADA

Summary Report: Service Level Expectations

Presented to the House of Commons Standing Committee on Public Accounts

In response to the June 2016 Report 9 – Chapter 4, Information Technology Shared Services, Fall 2015 Report of the Auditor General of Canada

November 2016

TABLE OF CONTENTS

SUMMARY OF SLES ESTABLISHED FOR ALL SSC SERVICES

The present report summarizes Service Level Expectations (SLEs) established by Shared Services Canada (SSC) for all its customer-facing services, as of September 2016. As part of SSC's Continual Service Improvement process, service catalogue content, including SLEs, is updated on an ongoing basis, as services evolve. The catalogue is intended to be a 'living document' and as such, the most recent content can be accessed at any time, via the SSC *Serving Government* website.[1]

CONCEPTS

The Treasury Board (TB) and Treasury Board of Canada Secretariat (TBS) have defined how federal organizations providing services must develop and report performance measures for their service provision levels. In October 2014, the new TB *Policy on Service* came into effect with requirements for setting service expectations with measurable levels of performance that customers can expect under normal circumstances. TBS has been assessing service provision practices and performance for several years through the Management Accountability Framework (MAF).

In compliance with the spirit and requirements of the TB policy and TBS instruments, SSC has defined service levels and associated performance targets for all its customer-facing services. In the private sector, such service performance expectations are defined, for IT services, within the *Information Technology Infrastructure Library* (ITIL) framework. The ITIL framework is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of organizations. As such, SSC has branded its measures of service performance as 'Service Level Expectations' or SLEs for the purposes of communicating with partners and customers, as well as reporting to TBS and Parliament on the policy requirements related to service standards.

Increasingly, customers are being engaged to support the establishment of SLEs. SSC Service Leads currently define SLEs by leveraging information from a range of sources including industry research, vendor consultation, historical knowledge of user requirements, and informal consultation with customers and SSC Account Teams. SSC is working to formalize documentation of customer requirements as part of each service's design phase. The catalogue is actively used by Account Teams and customer organizations, with overall positive feedback received to date regarding content.

INITIAL DEVELOPMENT AND EVOLUTION

SLEs were originally identified as part of the first phase of the development of the SSC Service Catalogue, initially published in March 2015. While standard catalogue entries were developed for all services, follow-on analysis of the information highlighted a lack of standardization of SLEs amongst services.

In order to improve consistency, a set of common SLEs required for all services was created (September 2015), based on internal consultation and industry research. These are:

[1] Shared Services Canada – Service Catalogue: http://service.ssc-spc.gc.ca/en/services (Accessed September 1, 2016)

1. Service Hours
2. Regular Scheduled Maintenance
3. Availability
4. Mean Time to Restore Service
5. External Vendor Support Hours
6. Request Fulfillment Duration

The definitions of these common SLEs and the detailed SLEs by service are provided in Appendix A and Appendix B, respectively.

SLEs at SSC may also be identified through vendor contracts, making the service provider responsible for meeting these SLEs.

SLEs and service catalogue content continue to evolve as service strategies, designs, and improvement initiatives are completed. New and/or service-specific SLEs will be added as required to improve alignment with industry standards.

INTEGRATION AND ENHANCED REPORTING

In November 2015, SSC's Service Catalogue included the SLEs for the Department's five priority services (Email, Mobile Devices, Videoconferencing, Application Hosting and the Government of Canada Wide Area Network or GC WAN) in compliance with the requirement of the TB *Policy on Service* for departments to have service standards for priority services available to clients.

SLEs for each of the Priority Services are detailed in Appendix C.

In March 2016, SSC launched a new and improved Service Catalogue accessible through its *Serving Government* site. Established to be the single source of information on services provided by SSC, the Catalogue's structure and main landing page have been revised to make services easier to find and each service description has been re-designed in a standard template for ease of use. As of September 2016, SLEs for all services are available via the Catalogue.

In April 2016, SSC issued the first *IT Health Systems* report, designed as a communication product for customers, also accessible via the *Serving Government* website. In addition to providing a snapshot of SLEs for selected services, this quarterly report contains information on key areas of IT system health performance (such as security, availability, reliability, and capacity) and on customer satisfaction.

Monthly *Operational Performance Reports* are provided to SSC Executives, which contain information on service levels and performance achieved for all customer-facing services. The status of each service going through the various phases of Service Lifecycle Management, including any considerations or action items related to SLEs, is also presented to governance committees on a monthly basis via a *Services Dashboard*.

APPENDIX A – DEFINITION OF COMMON SLES

1. **Service Hours**
   - Time period when the service should be available. (E.g.: 24x7, 365 days a year).

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

3. **Availability**
   - Availability is represented by the percentage of time, during service hours, that the service was performing its agreed function.
     - Percentage is calculated using the agreed service time, which excludes planned downtime (E.g.: maintenance), minus actual downtime.
     - Actual downtime will consider all service dependencies and the result will be based on the lowest common denominator that contributed to service unavailability (e.g. if a network failure resulted in a service being unavailable, the network availability is impacted).

4. **Mean Time To Restore Service (MTRS)**
   - The average time taken to restore an IT service or other configuration item after a failure. MTRS is measured from when the service or configuration item fails to when it is fully restored and delivering its normal functionality.

5. **External Vendor Support Hours**
   - Time period when support, provided directly to partners by an external vendor, should be available for the service.

6. **Request Fulfilment Duration**
   - Time period after receipt of a request containing correct and complete information in which the request should be fulfilled.

APPENDIX B – DETAILED SLES (BY SERVICE, ALPHABETICALLY)

APPLICATION HOSTING

(http://service.ssc-spc.gc.ca/en/services/app-hosting)

The Application Hosting service provides partners with a fully managed, secure, reliable and scalable multi-tier platform, including standardized application and database middleware, which allows partners to host and manage their data and business applications. The service provides a standard approach to using these platforms in non-production (development and test), pre-production and production environments, as required by partners' systems development life cycles.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	- Midrange: TBD - Mainframe: Following Service Management policies
Availability	99.5%
Mean Time to Restore Service (MTRS)	4 hours
External Vendor Support Hours	Not Applicable
Request Fulfillment Duration	Variable, based on the level of complexity of the request.

AUDIO CONFERENCING

(http://service.ssc-spc.gc.ca/en/services/teleconferencing)

Teleconferencing (Audio conferencing) enables multiple participants to collaborate by telephone anytime, anywhere, with or without operator assistance.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	The service performs upgrades periodically during weekend periods at a date to be determined by the supplier. A communique will be sent out in advance to the existing user community.
Availability	99.8%
Mean Time to Restore Service (MTRS)	Not Available
External Vendor Support Hours	24x7, 365/yr
Request Fulfillment Duration	Conference account confirmation of creation: Within 30 minutes.

BULK PRINT

(http://service.ssc-spc.gc.ca/en/services/bulk-print)

For Partners and clients who are printing and mailing forms or correspondence related to their programs to Canadian citizens or businesses, the Bulk Print service provides standardized and fully managed print-to-mail function to meet both high-volume and specialized print media requirements.

The service offers high-volume print and mailing capabilities from secure, centralized printing facilities.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	All maintenance activities can be carried out when the print center is in between jobs, or specific devices can be taken offline for maintenance, without affecting the availability of the service.
Availability	Minimum uptime for business applications and services: - Standard availability: 99.5% - High availability: Currently not available
Mean Time to Restore Service (MTRS)	Time to restore depends on the criticality of the outage.
External Vendor Support Hours	N/A
Request Fulfillment Duration	SSC evaluates each service request and determines the duration of fulfillment.

CONTACT CENTRE

(http://service.ssc-spc.gc.ca/en/services/contact-centre-infra)

Contact Centre provides all the contact/call handling, agent support, reporting, supervision and administration capabilities required to operate and manage a contact centre.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	No regularly scheduled maintenance windows identified. Software program changes are completed without service interruption. Notification for system or platform maintenance is a minimum of 10 business days in advance.
Availability	99.95% in any calendar month as per contract, except during scheduled downtime periods for routine maintenance work. Availability percentage excludes: Public Switched Telephone Network (PSTN) | Toll-Free network (TFN) | GC-Owned Networks.
Mean Time to Restore Service (MTRS)	- System functionality full recovery within 30 minutes (refers to IVR-Interactive Voice Response, ACD-Automatic Call Distribution). - Reporting functionality full recovery within 24 hours.
External Vendor Support Hours	Vendor trouble desk offers technical support 24 x 365.

Request Fulfillment Duration	The requested fulfillment duration varies depending on the complexity of the requested contact centre. Large, complex contact centres may take 6 months to one year to complete the service request.

DISTRIBUTED PRINT

(http://service.ssc-spc.gc.ca/en/services/distributed-print)

The Distributed Print service provides industry-standard access to network printing server capability within the Government of Canada network.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	Subject to monthly maintenance (short interruptions) to allow security updates to be applied; in such cases, the partner and client service desks will be informed.
Availability	Minimum uptime for business applications and services: - Standard availability: 99.5% - High availability: Currently not available
Mean Time to Restore Service (MTRS)	Time to restore depends on criticality of outage.
External Vendor Support Hours	Not Applicable
Request Fulfillment Duration	SSC will evaluate each service request and determine duration of fulfillment.

EMAIL

(http://service.ssc-spc.gc.ca/en/services/email)

Your.email@canada.ca enables individuals working for the Government of Canada to send and receive electronic mail messages and to manage a calendar, tasks, an address book and personal contacts. Each employee is entitled to one email account.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	Every Sunday EST 02:00 – 06:00
Availability	99.9%
Mean Time to Restore Service (MTRS)	4 hours
External Vendor Support Hours	24x7, 365/yr
Request Fulfillment Duration	99% of all SRs in a calendar month must meet: - Level 0: E-Enabled - Level 1: 3 FGWD ** - Level 2: 20 FGWD

*** FGWD = Federal Government working days*

External Credential Management
(http://service.ssc-spc.gc.ca/en/services/external-credential-management)

External Credential Management is a cyber authentication service provided by the Government of Canada to allow the public and businesses to securely conduct online business with various governmental programs and services. Use of this service is mandatory for Government of Canada departments and agencies.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	GCKey production: Sundays from 02:00 to 06:00 GCKey test environment: Wednesdays from 17:00 to 23:00 SecureKey Concierge Production: Sundays from 02:00 to 06:00 SecureKey Concierge User Acceptance Testing Environment: Thursdays from 17:00 to 21:00
Availability	GCKey Production Environment has a service availability of 99.8%. GCKey Testing Environment has a service availability of 95.0%. SecureKey Production Environment has a service availability of 99.8%. SecureKey User Acceptance Testing Environment is available 24x7, 365/yr with "best effort" support.
Mean Time to Restore Service (MTRS)	For GCKey: production 90 minutes, test environment 4 hours For SecureKey Concierge: production 4 hours
External Vendor Support Hours	GCKey Production and SecureKey Concierge Production: 24x7, 365/yr GCKey Test Environment: Monday to Friday from 07:00 to 19:00 SecureKey Concierge User Acceptance Testing Environment: Monday to Friday from 07:00 to 23:00
Request Fulfillment Duration	Negotiations and setup go through account management thus times vary by complexity of requirements.

File
(http://service.ssc-spc.gc.ca/en/services/file)

SSC File Services for partners currently provides file share services that are centralized, scalable, online storage solutions for unstructured data. It includes root share management, quota management, data migrations, data capacity trending and reporting. SSC is also working to provide future cloud-based file solutions for partners, which will allow for offline data, and data cross-platform synchronization among devices using a new and efficient way to manage unstructured data.

Service Hours	24x7, 365/yr – Services are fully operational and continuously monitored.
Regular Scheduled Maintenance	Regular scheduled maintenance is dependent on the underlying storage service provider.
Availability	Standard availability: 99.5% High availability: Currently not available
Mean Time to Restore Service (MTRS)	Recovery time objective (RTO) - Standard: 4 hours - High: Currently not available Recovery point objective (RPO) - Standard: 24 hours - High: Currently not available
External Vendor Support Hours	Support hours are dependent on the underlying storage service providers.
Request Fulfillment Duration	Standard User home drive – 2 weeks Standard Common drive – 2 weeks

FIXED LINE (LANDLINE) PHONES

(http://service.ssc-spc.gc.ca/en/services/mobile-dev-phones)

The Fixed Line (Landline) Phones service offers supplies and installs of telephone systems, services and devices, including: Voice over Internet Protocol (VoIP), Centrex, PBX and key systems.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	For Centrex: No regular scheduled maintenance. For VoIP (GENS): A regular scheduled maintenance occurs every 3 months affecting VoIP (GENS) Voice messaging system serving ESDC (Employment and Social Development Canada) and IRC (Immigration, Refugees and Citizenship Canada) only. Customers are notified in advance of maintenance (normally 2 weeks) via their Service Delivery Manager (SDM). During the 2 hours maintenance window, users will not be able to access their old voicemail messages.
Availability	99.999%
Mean Time to Restore Service (MTRS)	Targeted maximum time to restore the service is 4 business days (Maximum time and duration may be exceeded based on location and service requested).
External Vendor Support Hours	Not Applicable
Request Fulfillment Duration	Targeted maximum request fulfillment duration is 8 business days depending on complexity of request (Maximum time and duration may be exceeded based on location and service requested).

GC LAN (Local Area Network)
(http://service.ssc-spc.gc.ca/en/services/network-infra)

The Government of Canada Local Area Network (LAN) service helps partner and client organizations with the interconnection of network segments in building and campus environments. The service and its offerings provide a reliable means of transport for converged communication services, such as voice/data/video, IP telephony, instant messaging and conferencing.

Note: *for Cabling see Cabling - Service Level Metrics (http://service.ssc-spc.gc.ca/en/services/network-infra/gcnetlan-admin/cabling-service-levels)*

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	All regular scheduled maintenance is sub-service, site- and Partner-specific. Please contact your organization's help desk.
Availability	Not applicable
Mean Time to Restore Service (MTRS)	Primary Service Areas - Regular: MTTA (mean time of arrival) 1 day / MTTR (mean time to resolution) 3 days - Priority: MTTA 4 hours / MTTR 2 days - Emergency: MTTA 2 hours / MTTR 4 hours Remote Service Areas - Regular: MTTA 1 day / MTTR 3 days - Priority: MTTA 4 hours / MTTR 2 days - Emergency: MTTA 2 hours / MTTR 4 hours
External Vendor Support Hours	Not applicable
Request Fulfillment Duration	Primary Service Areas - Regular – 5 work days - Priority – 3 work days - Emergency – 1 work day Remote Service Areas - Regular – 8 work days - Priority – 5 work days - Emergency – 2 work days

GC WAN (Wide Area Network)
(http://service.ssc-spc.gc.ca/en/services/network-infra)

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

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	Site and/or partner specific
Availability	From 99.3% to 99.999% (site specific) Availability is site-specific. Service level objectives range from 99.3%, up to 99.999% for most national locations. International locations or locations with satellite service have objectives which range from 99.8% up to 99.999%.
Mean Time to Restore Service (MTRS)	Site and/or Partner specific
External Vendor Support Hours	24x7, 365/yr
Request Fulfillment Duration	Site and/or Partner specific

HIGH PERFORMANCE COMPUTING

(http://service.ssc-spc.gc.ca/en/services/high-perf-comp)

The High-performance Computing service provides a fully managed platform for extreme performance computing needs, such as intermittent computing or steady-state heavy computing in both research and production environments.

Service Hours	Standard availability: Government business hours High availability: 24x7, 365/yr – Services are fully operational and continuously monitored.
Regular Scheduled Maintenance	As needed. The service is maintained with sufficient redundancy to allow transparent maintenance.
Availability	Standard availability: 96.0% High availability: 98.0% Note: Only critical and high-priority incidents are measured against this service level.
Mean Time to Restore Service (MTRS)	RTO: maximum time allowed to restore a service to its operational state in the event of an outage. Recovery time objective (RTO): - Standard – 4 hours - High – 30 mins RPO: maximum transaction/data loss in the event of an incident. Recovery point objective (RPO): - Standard – 24 hours - High – up to 4 hours
External Vendor Support Hours	Not applicable
Request Fulfillment Duration	Under review

INTERNET

(http://service.ssc-spc.gc.ca/en/services/network-infra)

The Government of Canada Network (GCNet) Internet service provides connectivity for GCNet users to access the Internet and for the public to access Government of Canada websites.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	Enterprise service: dependent on GC WAN service. Local Internet Access Service: none, this is a fully managed service provided by commercial service providers.
Availability	Enterprise service: 99.5% Local Internet Access Service: standard availability objectives for: - Symmetrical service 99.5% - Asymmetrical service 98%
Mean Time to Restore Service (MTRS)	Enterprise service: 4 hours Local Internet Access Service: - Symmetrical services – 4 hours - Asymmetrical service – 24 hours
External Vendor Support Hours	Enterprise service: SSC receives 24x7 support from the vendors. Local Internet Access Service: 24x7 support between the help desk and vendors.
Request Fulfillment Duration	Depends on the location and requested service; duration varies from 30 to 60 business days.

MICROCOMPUTERS

(http://service.ssc-spc.gc.ca/en/services/microcomputers)

The Microcomputers service provides access to standing offers for computers and computer-related peripherals and systems, including: desktop computers, notebooks, hybrid tablets and specialized devices.

Service Hours	Monday to Friday, 8:00 a.m. to 4:00 p.m. EDT, excluding statutory holidays.
Regular Scheduled Maintenance	Not applicable
Availability	99.9%
Mean Time to Restore Service (MTRS)	Not applicable
External Vendor Support Hours	Not applicable

Request Fulfillment Duration	Emergency Contracts – defined in accordance with the TB Contracting Policy and Notice CPN 2007-4 – immediate. Orders using existing SSC Methods of Supply and Catalogues. Such as: Call-ups against a standing offer, or Orders against SSC Virtual Inventory – up to 10 days. Technical Exceptions – case by case. RVDs are run on a 2 months cycle and deadlines for requests are published.

MOBILE DEVICES

(http://service.ssc-spc.gc.ca/en/services/mobile-dev-phones)

The Mobile Devices service provides cellular phones, smartphones and cellular data devices, along with their service plans. Specialized solutions for emergency-response personnel and senior management personnel on travel status are also available.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	None
Availability	Wireless & Voice mail: 99.95% in any calendar month as per contract.
Mean Time to Restore Service (MTRS)	Not Applicable
External Vendor Support Hours	24x7, 365/yr
Request Fulfillment Duration	5 business days

MYKEY

(http://service.ssc-spc.gc.ca/en/services/mykey)

The myKEY service is an internal credential management (ICM) service that facilitates authentication for secure access to applications and Government of Canada networks. It is used to eliminate potential deniability of transactions using digital signatures and to facilitate the exchange of encrypted email and documents for Protected B information. It is also used for authentication between users, applications and devices (e.g. Compensation Web Applications (CWA) and Government of Canada Secure Remote Access (GCSRA)).

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	Core myKEY maintenance periods are typically one Sunday in each month, from 05:00 to 09:00.
Availability	99.5%, excluding monthly maintenance, with the exception of Online Registration and Credential Administration (ORCA) and myKEY LOGIN.

Mean Time to Restore Service (MTRS)	4 hours
External Vendor Support Hours	Not applicable
Request Fulfillment Duration	Completion target for an LRA myKEY Certificate request is 48 to 72 hours.

NETWORKING EQUIPMENT

(http://service.ssc-spc.gc.ca/en/services/networking-equipment)

The Networking Equipment service provides the Government of Canada with the ability to purchase telecom networking equipment, as well as services for the installation and maintenance of the networking equipment. It offers a single point of access for the purchase of up-to-date telecom networking equipment from major suppliers at volume-based prices.

Service Hours	24x7, 365/yr (Legacy NESS web portal); Analysts available to review requirements Monday to Friday, 7:00 a.m. to 4:00 p.m. EDT/EST, excluding statutory holidays.
Regular Scheduled Maintenance	None
Availability	99% (Legacy NESS web portal uptime)
Mean Time to Restore Service (MTRS)	Not applicable
External Vendor Support Hours	Varies per vendor and per selected service (For enquiries related to support hours contact the IPS Team).
Request Fulfillment Duration	Purchase request: - 1 month typical period until contract signature, if all required documents are included. - Reseller delivery period is 2 to 30 days. Maintenance request: - 1 month typical period until coverage is active. - Contract with new vendor requires 2 to 3 months.

PRINTING PRODUCTS

(http://service.ssc-spc.gc.ca/en/services/printing-products)

Workplace Technology Devices (WTD) Printing Products provide access to standing offers for WTD printing products and printing-related devices and services.

Service Hours	Monday to Friday, 8:00 a.m. to 4:00 p.m. EDT, excluding statutory holidays.
Regular Scheduled Maintenance	Not applicable
Availability	99.9%
Mean Time to Restore Service (MTRS)	Not applicable

External Vendor Support Hours	Not applicable
Request Fulfillment Duration	Emergency Contracts – defined in accordance with the TB Contracting Policy and Notice CPN 2007-4 – immediate. Orders using existing SSC Methods of Supply and Catalogues. Such as: Call-ups against a standing offer, or Orders against SSC Virtual Inventory – up to 10 days. Technical Exceptions – case by case. RVDs are run on a 2 months cycle and deadlines for requests are published.

SATELLITE

(http://service.ssc-spc.gc.ca/en/services/network-infra)

The Satellite services provide satellite-based telecommunications services including fixed and mobile solutions, both nationally and internationally.

Service Hours	Fixed: 24x7, 365/yr Mobile: 24x7, 365/yr
Regular Scheduled Maintenance	Fixed: - VSAT Enterprise: As required and communicated by the supplier and performed outside the business hours. - Enterprise Point-to-Point (Ottawa-Iqaluit; Ottawa-Resolute): As required and communicated by the supplier and performed outside the business hours. - Scheduled maintenance does not apply to other FSS services that are strictly space segment bandwidth. Mobile: - MSAT: 2:00 am to 4:00 am on Sundays. - Inmarsat: As required and communicated by the supplier and performed outside the business hours. - Iridium: As required and communicated by the supplier and performed outside the business hours. - Globalstar: As required and communicated by the supplier and performed outside the business hours.

Availability	Fixed: - VSAT Enterprise: 99.3% to 99.8% network availability (annual) - Enterprise Point-to-Point (Ottawa-Iqaluit; Ottawa-Resolute): 99.3% network availability (annual) - Other FSS services which are strictly space segment have consistent service availability closer to 100% Mobile: - MSAT: 99.9% network availability (annual) - Inmarsat: 99.8% network availability (annual) - Iridium: 95% network availability (annual) - Globalstar: 95% network availability (annual)
Mean Time to Restore Service (MTRS)	Fixed: These times are variable dependent on the geographical locations of the remote satellite earth stations. It varies anywhere from 4 hours to 48 hours for most cases. Mobile: Not applicable since mobile satellite terminals are not subject to maintenance.
External Vendor Support Hours	Fixed: 24x7 Mobile: 24x7
Request Fulfillment Duration	Fixed: Varies, depends on a case-by-case basis. Most cases the time is within 30 days, inclusive of funds commitment and order processing. Mobile: Varies depending on request from an activation requiring a 2 hour turnaround to a completely new installation requiring 30 days.

SECURE REMOTE ACCESS

(http://service.ssc-spc.gc.ca/en/services/secure-remote-access)

The Government of Canada Secure Remote Access (GCSRA) service provides users with the ability to securely transmit and receive information from remote client workstations or remote gateways while maintaining the availability, confidentiality and integrity of the data.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	Maintenance outages are planned in advance and coordinated with the client department; usually outside of business hours. There are no regular maintenance windows.
Availability	99.9%
Mean Time to Restore Service (MTRS)	Maximum time to restore service on site will be four hours. Maximum time to restore service to remote sites will be 24 hours.
External Vendor Support Hours	Pre-authorized individuals within SSC may contact the Bell Help Desk 24x7.
Request Fulfillment Duration	40 FGWD **

*** FGWD = Federal Government working days*

SOFTWARE PROVISIONING
(http://service.ssc-spc.gc.ca/en/services/software-provisioning)

Software Provisioning provides an end-to-end request fulfillment process for WTD software, i.e. single point of contact for WTD base software; end-to-end process, from request to order fulfillment (create new orders, view existing orders, search orders); and access to enterprise software agreements.

Service Hours	Monday to Friday, 8:00 a.m. to 4:00 p.m. EDT, excluding statutory holidays.
Regular Scheduled Maintenance	99.9%
Availability	Same as email service (email availability is 99.9%) as there is a dependency on the email service.
Mean Time to Restore Service (MTRS)	Not applicable
External Vendor Support Hours	Not applicable
Request Fulfillment Duration	- Net new product request – 10 days. - Amend existing contract (add to existing base, assumes SSC has transferred the contract) – 10 days. - Draw from available pool of licenses – 2 days.

TOLL-FREE VOICE
(http://service.ssc-spc.gc.ca/en/services/toll-free-voice)

Toll-free Voice provides callers with free long distance (1-800) access to Government of Canada departments and agencies across Canada.

Service Hours	The Toll-free service is available and supported 24x7, 365/yr. Service hours may vary by partner depending on the hours of operation provided by the local helpdesk.
Regular Scheduled Maintenance	No pre-defined maintenance window has been identified for this service.
Availability	99.99%
Mean Time to Restore Service (MTRS)	Information not available at this time.
External Vendor Support Hours	The vendor`s support desk operates 24x7, 365/yr.
Request Fulfillment Duration	Simple orders are typically completed within 3-5 federal government working days and are processed during vendor’s order desk normal hours of operations. Complex orders may take additional time to complete.

VIDEOCONFERENCING

(http://service.ssc-spc.gc.ca/en/services/videoconferencing)

Videoconferencing (VC) systems enable you to conduct two-way video calls. With SSC's videoconferencing service, you can hold video meetings interdepartmentally and externally.

Service Hours	24x7, 365/yr; Service business and support hours are 8 a.m. to 4 p.m. on regular work days.
Regular Scheduled Maintenance	None - Maintenance performed outside of business hours as required.
Availability	99%
Mean Time to Restore Service (MTRS)	2 business days
External Vendor Support Hours	Not Applicable
Request Fulfillment Duration	5 business days

WEB CONFERENCING

(http://service.ssc-spc.gc.ca/en/services/web-conferencing)

Web conferencing (WebEx) enables you to conduct a conference over the Web. Content from the screen of the meeting host, or from a participant's computer, is displayed on all participants' computers. This includes documents, applications, browsing sessions and live desktop video.

Service Hours	24x7, 365/yr
Regular Scheduled Maintenance	The Web conference service performs upgrades periodically during weekend periods at a date to be determined by the supplier. A communiqué will be sent out in advance to the existing user community.
Availability	99.8%
Mean Time to Restore Service (MTRS)	Not available
External Vendor Support Hours	24x7, 365/yr
Request Fulfillment Duration	Conference account confirmation of creation: within 30 minutes.

APPENDIX C – SLES FOR PRIORITY SERVICES

List of SSC's Priority Services (in alphabetical order)	Service Level Expectations					
	Service Hours	Regular Scheduled Maintenance	Availability	Mean Time to Restore Service (MTRS)	External Vendor Support Hours	Request Fulfillment Duration
Application Hosting	24x7, 365/yr	Midrange: TBD Mainframe: Following Service Management policies	99.5%	4 hours	Not Applicable	Variable, based on the level of complexity of the request
Email	24x7, 365/yr	Every Sunday EST 02:00 - 06:00	99.9%	4 hours	24x7, 365/yr	99% of all SRs in a calendar month must meet: * Level 0: E-Enabled Level 1: 3 FGWD ** Level 2: 20 FGWD
GC WAN (Wide Area Network)	24x7, 365/yr	Site and/or Partner specific	From 99.3% to 99.999% (site specific)	Site and/or Partner specific	24x7, 365/yr	Site and/or Partner specific
Mobile Device	24x7, 365/yr	None	99.95% (Wireless & Voice mail; in any calendar month as per contract)	Not Applicable	24x7, 365/yr	5 business days
Videoconferencing	24x7, 365/yr (Service business and support hours are 8 a.m. to 4 p.m. on regular work days)	None - Maintenance performed outside of business hours as required	99%	2 business days	Not Applicable	5 business days

** Vendor contracts are based on Maximum Time to Restore (as opposed to the common SLE based on Mean Time To Restore Service)*

*** FGWD = Federal Government working days*

Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Government of Canada Information Technology

Strategic Plan

2016 – 2020

Service – Security – Value – Agility

Table of Contents

June 22, 2016

Message from the Chief Information Officer of the Government of Canada

The Government of Canada's Information Technology Strategic Plan sets out the four-year strategic direction for information technology (IT) in the federal government. In responding to government priorities and current challenges, the plan charts the path forward for IT from a whole-of-government or "enterprise" perspective, positioning the government to manage and use IT as a strategic asset, in innovative ways, to deliver better programs and services and ultimately value to Canadians.

Developing this plan provided the opportunity to assess our progress and reconfirm the Government of Canada's commitment to the continued enterprise transformation of IT. The goal of this transformation is to enable improved and easier access to government services by business and individuals in ways that meet their expectations for a responsive, modern and secure digital government. In developing this plan, we also looked at what other jurisdictions are doing to organize internal capacity to drive innovation in digital services. We will consider various models as we explore new approaches to utilize internal capacity to meet our current and future needs.

At its core, the plan is intended to guide federal organizations and the IT community on IT priority setting and decision-making. This is why it includes actions to strengthen the current enterprise governance, a key to our success going forward.

This plan will also inform Shared Services Canada's (SSC's) direction and priorities as SSC revises and implements the plan to renew the Government of Canada's IT infrastructure. The strategic actions outlined in this plan include both current commitments and activities, as well as new enterprise directions, some of which may require additional approvals or funding to be fully implemented. Regardless of their status, the directions outlined provide important guideposts for departments and agencies as they develop their individual IT plans and prioritize their IT investments.

Not all actions set out in this plan are expected to be completed by 2020. Neither is it expected that all departments and agencies will implement these actions within the same time frame. Some actions may not be applicable or appropriate for all departments, most notably small departments and agencies. Deputy heads, in consultation with the Treasury Board of Canada Secretariat (TBS), will take this into consideration when implementing the strategic plan.

I extend my sincere thanks to the Government of Canada's Chief Information Officer (CIO) community and many other federal partners who helped us build this strategic plan. Through careful planning and cooperation within the Government of Canada enterprise, we can achieve the IT vision and meet the strategic goals outlined in this document.

John Messina
Chief Information Officer of the Government of Canada

Executive Summary

Traditionally, government organizations have set up and run their own IT infrastructure and services in order to carry out their respective mandates. Over the last few years, the Government of Canada has taken the first steps to transform its approach to IT infrastructure and service delivery. These steps have included initiatives to transform the "back office" services provided to employees, such as human resources, financial services and records management, and to provide IT infrastructure, email, data centres and network services across government through Shared Services Canada.

This IT strategic plan builds on the lessons learned from these initiatives, and seizes on the opportunities created by technologies such as social media, mobile devices, analytics and cloud computing to fully maximize the benefits of an enterprise approach to IT. This plan will deliver to Canadians the kind of government they expect – one that is open and transparent yet safeguards their personal information, one that delivers effective and responsive programs and services while being fiscally prudent, and one that makes decisions based on sound evidence while seeking meaningful engagement and collaboration with Canadians and other stakeholders.

To deliver on these citizen expectations, employees require modern and effective tools for their day-to-day work. They demand a modern workplace with digital tools that are integrated, collaborative and efficient. Along with these requirements, constantly evolving technology and the need to protect vital data and information from malicious cyber threats, make it essential that we renew our aging and mission-critical IT systems. At the same time, we must balance the growing demand for IT services with realistic capacity limitations.

Building on these key drivers, the overarching goals of ***service, security, value*** and ***agility*** set the direction for the strategy. The Government of Canada is committed to responsive and innovative IT services that meet business needs and enhance the end-user experience, to a secure and resilient enterprise infrastructure that enables the trusted delivery of programs and services, to smart investments across the board that ensure high-value and cost-effectiveness, and to an agile, connected and high-performing workforce with modern tools. Four strategic areas of action will achieve these goals over the next four years and beyond. Each area of focus, *Service* IT, *Secure* IT, *Manage* IT, and *Work* IT details specific actions and activities that are currently underway or that represent new enterprise directions.

The first, ***Service* IT**, calls for the use of cloud computing, information-sharing platforms, and technologies and tools to manage service delivery and improve client satisfaction. These actions are necessary in order to develop a modern, reliable and sustainable IT infrastructure that allows for the secure sharing of information. This in turn will ultimately result in better internal services for government employees and improved external services for Canadians and other users.

The second area, ***Secure* IT**, focuses on layered defences to reduce exposure to cyber threats, increased awareness and understanding to proactively manage these threats, and protective measures to enable the secure processing and sharing of data and information across government. These actions will ensure that Canadians and others who access online services trust the government with their personal information.

The third area, ***Manage* IT** presents a strengthened governance approach, the evolution of IT management practices, process and tools and a focus on innovation as well as sustainability. Implementing these strategic actions will ensure that IT investments are sustainable, take

advantage of economies of scale, and demonstrate value by helping departments deliver on their mandates.

The fourth area, ***Work* IT**, introduces actions to build a high-performing IT workforce and a modern workplace that provides public service employees with the tools they need to do their jobs. This is vital because the Government of Canada's employees are its greatest asset when it comes to delivering the kind of government that Canadians want.

Progress towards achieving the strategic goals outlined in the IT strategic plan will be tracked, evaluated and reported. As it evolves, the government's IT strategic plan will require the government to make investment choices. It will be reviewed yearly to ensure it stays up to date and relevant, supported by an implementation roadmap to track and report on progress (Appendix A). Departments and agencies through their investment plans, will detail how this enterprise approach will be implemented in their organization.

With this strategic plan, the Government of Canada has set out a clear path to getting the maximum benefit out of the money it spends on IT. Implementing this agenda is crucial to ensuring that the Government of Canada is ready and able to meet the needs and expectations of Canadians in the years ahead.

Introduction

IT services in the Government of Canada are delivered by **17,000 IT professionals** working in more than **1,500 government locations** across Canada and around the world.

The government's **total annual spending on IT is $5 billion**, an amount that has been stable over the past 5 years.

Government departments spend **$3 billion** annually on applications, computing devices and IT program management.

The Government of Canada is made up of more than 100 separate organizations that deliver a broad range of programs and services to individuals and businesses in Canada and abroad. IT supports the government in delivery of these programs and services. In the past, many operated their own IT infrastructure and services to carry out their respective mandates. Increasingly, the disadvantages of this approach have become apparent. Inefficiency, duplication and IT-systems incompatibility have hindered the ability of government decision-makers to get the high-quality, real-time information they need to deliver excellent results.

A whole-of-government, or "enterprise" approach to IT infrastructure and service delivery is addressing these short-comings. The responsibility for delivering IT services to core departments and agencies is now shared between central providers such as Shared Services Canada (SSC) and Public Services and Procurement Canada (PSPC). Cyber and IT security is the shared responsibility of SSC, the Communications Security Establishment (CSE) and Public Safety Canada. The Chief Information Officer Branch (CIOB), of Treasury Board Secretariat (TBS) supports Treasury Board by developing strategy, setting government-wide policy for IT and cybersecurity, and providing implementation guidance.

Today's business environment continues to be characterized by disruption and the imperative to do more, faster, with less. In our digital era, individuals, business and others who interact with government have high standards for the services they receive. The Government of Canada is transforming how government works so that it better reflects the values and expectations of its clients.

This IT strategic plan supports the continued transformation to enterprise IT infrastructure and service delivery and proposes to address these and other challenges by responding to the following key drivers:

- Citizen expectations
- Workplace and workforce evolution
- Security
- The enterprise approach
- Aging IT and sustainability

Citizen expectations

Canadians want and deserve technology that provides the best service to them, when and where they need it, and in a client-centric manner. They want to be assured that departments and agencies are using the best available data to make evidence-based decisions with respect to policies, programs and services that affect everyone. They value government that is open with its data and other business information yet protects their privacy.

Workplace and workforce evolution

Internal clients, including employees, expect modern and effective tools that connect up to make their day-to-day work efficient and provide value-added to their efforts. They demand a digital experience that is optimized, integrated and diversely client-centric. Employees in a modern workplace need digital tools that promote collaboration, information sharing and increased productivity.

Security

Cybersecurity is an ever-evolving aspect of any information technology strategy. While bringing important opportunities, the consolidation of systems leads to a greater attack surface that requires enhanced security measures to minimize risks. Inconsistent management of government networks and the security profiles of government endpoint devices – computer devices capable of connecting to the Internet – also has the potential to increase the risk of cyber-attack.

The enterprise approach

Sharing our infrastructure, and using common IT solutions to meet common needs, is one part of leveraging technology in a whole-of-government, or enterprise, approach, along with addressing security, privacy, accessibility, and open information requirements.

For IT users, it will be important to ensure a consistent end-user experience government-wide, regardless of geographical location. Issues of latency, bandwidth, security, infrastructure and other considerations need to be taken into account. As well, the complexity of IT-enabled projects is increasing as we move toward a more horizontal delivery model. Authoritative governance is needed to make enterprise decisions about IT investments.

Aging IT and sustainability

There is a continued need to renew the government's aging and mission critical IT infrastructure and systems that are at risk of breaking down. IT infrastructure transformation is proceeding slower than anticipated; complexity of the task has caused some delays and procurement is taking longer than planned. Funding pressures are arising, in part, from stronger than forecasted growth in demand. Chronic under investment puts the government's ability to deliver some essential services to Canadians at risk. While progress has been made to rationalize applications, current system health indicators signal more work is needed to address this risk.

The Vision

The provision of secure, agile and reliable IT services delivers improved productivity and streamlined, high quality government services that are simpler and easier to access, where and when our clients want them.

Aging IT risks have been reduced through the completion of the IT infrastructure transformation and implementation of models and processes to ensure sustainable funding to address IT renewal. IT platforms that are the backbone for information sharing, big data analytics and collaboration, enable the use of high quality government data to inform decisions and identify innovative approaches to public policy. The use of enabling technologies such as cloud computing and social media offer more ways to engage with Canadians and others.

Through proactive measures, the government has reduced the threat surface of internet-connected networks and improved controls regarding access to government-held information. Enhancing government network and system security ensures that Canadians and others assessing online services can trust the government with their personal information.

IT investment that is targeted at business priorities drives greater efficiency and encourages innovation by government and third parties. Better management of IT investment maximizes

value and reduces service delivery costs, enabling the government to respond more rapidly to emerging issues.

The government is served by a high performing, strategically minded IT workforce who enjoy exciting career opportunities in the federal government. The Public Service is highly connected, and technology integrates seamlessly into daily work life. IT allows people to work smarter and solve problems more effectively by providing secure, agile and reliable systems and tools for information sharing, collaboration, and innovation.

Mission Statement

Federal information technology professionals are strategic partners within our organizations, providing excellence in IT services and delivering secure, reliable and agile technology. Working collaboratively with stakeholders and across government, our efforts add value in the workplace and contribute to better programs and services for Canadians.

Guiding Principles

Principle 1: Enable a modern workplace: Anywhere, anytime, with anyone

The Government of Canada strives to be an innovative organization that provides its employees with modern technology that supports information sharing, collaboration, and that will attract, retain and encourage public servants to work smarter, be innovative, greener and healthier so that they may better serve Canadians.

Principle 2: Think “enterprise” first

Where an enterprise solution exists to meet a common business need, departments and agencies should stop investing in departmental legacy versions and refocus efforts, resources and funds on becoming ready to adopt the enterprise solution and on accelerating its delivery.

Principle 3: Use cloud computing services

Departments and agencies should explore Software as a Service (SaaS) cloud computing services before developing solutions in-house. Cloud computing services are to be procured through SSC, which will act as the Government of Canada’s cloud service broker.

Principle 4: Meet common business needs through shared solutions

Departments and agencies should actively seek out opportunities to pool resources inter-departmentally to address common business needs.

Principle 5: Examine options

Where an enterprise solution to meet a common business need does not exist, departments and agencies should examine potential solutions taking into consideration total cost of ownership, ability to meet current and future business requirements, interoperability and assessing internal capacity.

Strategic Goals

The overarching strategic goals of ***service***, ***security***, ***value***, and ***agility*** along with the mission statement set the direction for the IT strategic plan. The Government of Canada is committed to responsive and innovative IT services that meet business needs and enhance the end-user experience, to a secure and resilient enterprise infrastructure that enables the trusted delivery of programs and services, to smart investments across the board that ensure high-value and cost-effectiveness, and to a connected and high-performing workforce with modern tools.

Strategic goal #1: Service

A responsive and innovative IT service that meets business needs and enhances the end-user experience

- Adopt emerging technology to improve service delivery
- Continue enterprise-wide approach to delivering IT services
- Provide public service employees access to modern self-service tools and applications

Strategic goal #2: Security

A secure and resilient enterprise infrastructure that enables the trusted delivery of programs and services

- Enhance security measures to minimize risk
- Provide more consistent management of government networks
- Protect personal and sensitive information

Strategic goal #3: Value

Smart investments that are both high in value and cost-effective

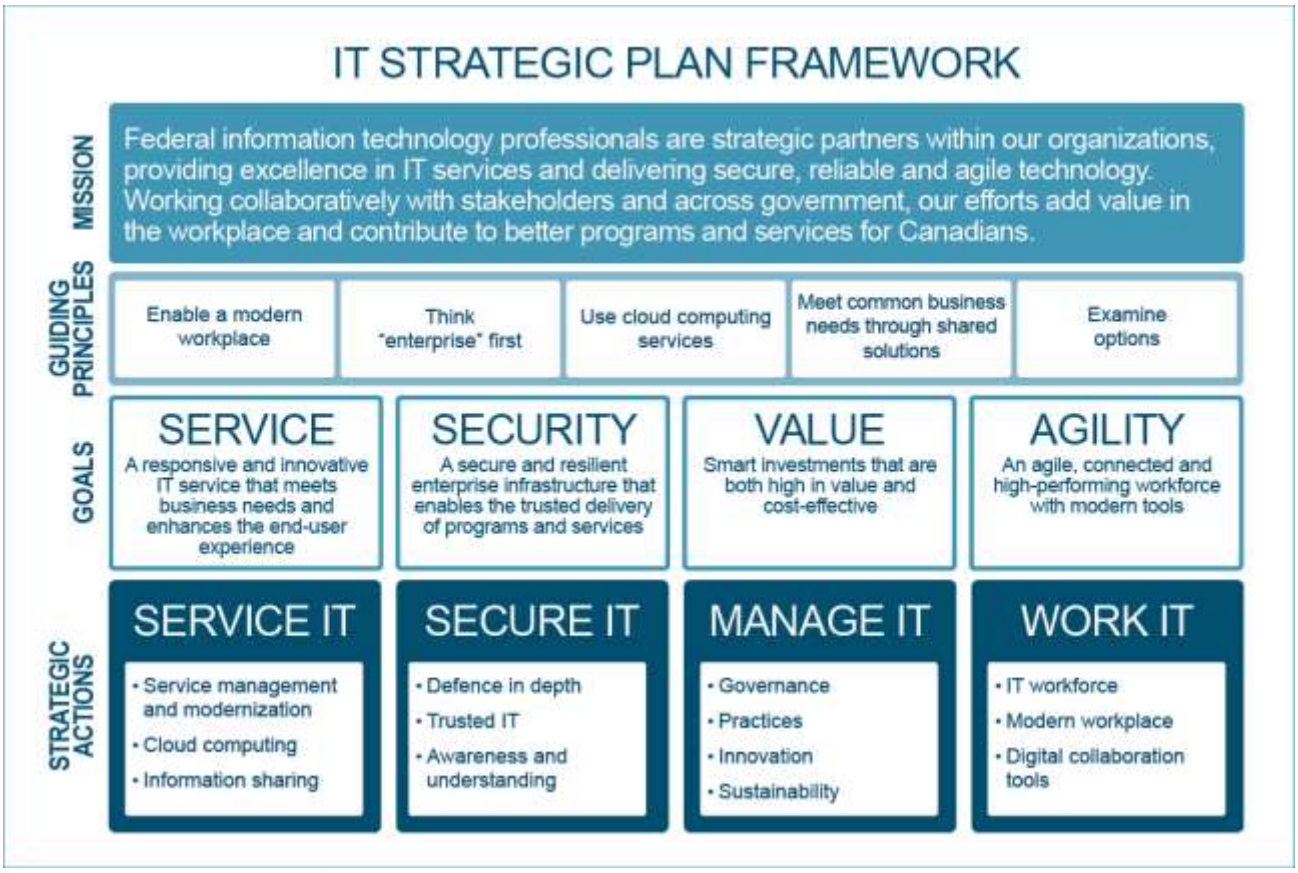
- Encourage collective use of resources, tools, processes and systems
- Develop enterprise-wide solutions to address common business needs
- Ensure sustainability of IT systems and infrastructure

Strategic goal #4: Agility

An agile, connected and high-performing workforce with modern tools

- Attract and retain highly-skilled and diverse IT talent
- Provide a technologically advanced workplace
- Promote digital literacy and collaboration

Four key areas of action, *Service* IT, *Secure* IT, *Manage* IT, and *Work* IT, and have been identified to achieve these strategic goals over the next four years and beyond. Each of these four key areas detail the specific actions and activities required to deliver results under the goals of service, security, value and agility. The IT strategic plan framework is illustrated below.


IT STRATEGIC PLAN FRAMEWORK
MISSION
Federal information technology professionals are strategic partners within our organizations, providing excellence in IT services and delivering secure, reliable and agile technology. Working collaboratively with stakeholders and across government, our efforts add value in the workplace and contribute to better programs and services for Canadians.
GUIDING PRINCIPLES
Enable a modern workplace
Think "enterprise" first
Use cloud computing services
Meet common business needs through shared solutions
Examine options
GOALS
SERVICE
A responsive and innovative IT service that meets business needs and enhances the end-user experience
SECURITY
A secure and resilient enterprise infrastructure that enables the trusted delivery of programs and services
VALUE
Smart investments that are both high in value and cost-effective
AGILITY
An agile, connected and high-performing workforce with modern tools
STRATEGIC ACTIONS
SERVICE IT
• Service management and modernization
• Cloud computing
• Information sharing
SECURE IT
• Defence in depth
• Trusted IT
• Awareness and understanding
MANAGE IT
• Governance
• Practices
• Innovation
• Sustainability
WORK IT
• IT workforce
• Modern workplace
• Digital collaboration tools

SERVICE *IT*

A responsive and innovative IT service that meets business needs and enhances the end-user experience

Service *IT* focuses on developing a modern, reliable, interoperable and sustainable IT infrastructure that allows for secure sharing of information, ultimately resulting in better internal services for government employees and improved external services for Canadians. Table 1 (below) shows the strategic actions that are currently underway, and those that represent new enterprise directions which may require additional approvals or funding to be implemented.

ACTIONS UNDERWAY	FUTURE ACTIONS
Develop IT service portfolios and catalogues	Implement enterprise IT service management tools
Report on key areas of IT system health performance	Offer private cloud services
Complete data centre consolidation and modernization	Introduce a government mobile applications store
Complete network consolidation	Introduce a government API store
Complete government email consolidation	Implement a platform for external collaboration
Adopt cloud computing services	Advance analytics capabilities
Establish a cloud service broker	
Offer public cloud services	
Build a platform for enterprise interoperability	

Service management and modernization

The more open, transparent and integrated government programs and services become, the more they will depend on IT to deliver secure and reliable services that meet agreed upon expectations.

Develop IT service portfolios and catalogues

An IT service portfolio describes services in terms of business value, including:

- A list of services
- A description of how they are bundled or packaged
- The benefits they deliver

An IT service catalogue is a list of available technology resources and offerings within an organization. It is a tactical, operational tool that is intended to make it easier for clients to request IT services on a day-to-day basis.

SSC and PSPC will develop IT service portfolios and service catalogues that clearly articulate enterprise service expectations for the services they provide, including:

- Roles and responsibilities
- Service targets
- Associated reporting commitments

SSC and PSPC will price their services to facilitate the introduction of:

- Chargeback models

- Price comparisons of external service providers
- The adoption of cloud services

With respect to IT security, SSC will establish expectations and provide the necessary information to partners for the IT infrastructure that it manages.

Report on key areas of IT system health performance

Key performance indicators that focus on operational excellence and delivery are critical tools in managing the delivery of IT services. Departments and agencies will put in place metrics for monitoring client satisfaction and key areas of IT system performance (e.g., security, availability, reliability and capacity).

For the services they provide, SSC and PSPC will:

- Set enterprise-wide service-level expectations in collaboration with departments and agencies
- Report to departments and agencies on performance based on these expectations
- Engage their clients to resolve issues if service levels fall below targets

Implement enterprise IT service management tools

IT service management (ITSM) refers to an organization's planning, delivery, operations and control of IT services offered to clients. Departments and agencies traditionally have implemented their own ITSM tools. These tools are expensive to implement and maintain, and the diversity of tools affects overall ITSM efficiencies. Moreover, service request and trouble tickets do not flow easily within and between organizations.

SSC will put in place enterprise ITSM tools and make them available to all departments and agencies. This will bring consistency to the practice of ITSM and, more importantly, reduce the cost and delays of fulfilling service requests.

Complete data centre consolidation and modernization

The Government of Canada operates over 500 aging data centres that support mission-critical and non-mission-critical business functions. Consolidating these data centres into fewer modern and secure data centre services is the most cost-effective way to address the government's "rust out" issue. These enterprise data centres will be designed with the ability for backup and retention, as part of disaster recovery plans and in support of business continuity.

The Government of Canada operates over 500 aging data centres that support mission-critical and non-mission-critical business functions. Consolidating these data centres into fewer modern and secure data centre services is the most cost-effective way to address the government's "rust out" issue. These enterprise data centres will be designed with the ability for backup and retention, as part of disaster recovery plans and in support of business continuity.

SSC will enable the migration of departmental legacy applications to segregated partner-specific locations (called enclaves) within the new enterprise data centres. This migration will accelerate the closure of aging data centres, enhance data security and minimize the financial and business impact to organizations.

To ease the demand for data centre capacity, departments will reduce the number of back office applications to be migrated. The extent to which the government leverages external cloud service providers could also reduce the requirement for data centre capacity.

Successfully consolidating data centres depends on departments' readiness to prepare their applications for migration within prescribed timeframes. Departments and agencies will work with SSC and other government and external partners to ensure that:

- Mission-critical and other applications are in appropriate environments
- These applications are supported with appropriate technologies and procedures to ensure their availability

Complete network consolidation

To streamline and modernize the government's network infrastructure and services, SSC will eliminate unused phone lines and migrate departments from outdated and costly legacy phone systems to wireless devices and VoIP service.

SSC will also work with departments and agencies to:

- Consolidate the 50 existing SSC partner wide-area networks into a single enterprise network
- Establish shared network infrastructure in office buildings that house multiple departments
- Secure and reduce the number of connections to the Internet

Complete government email consolidation

Departments and agencies have traditionally operated their own email systems, leading to business and cost inefficiencies. Departments and agencies will reduce the size of employees' mailboxes. SSC and departments and agencies will work to complete the task of consolidating email services to a common system.

Cloud computing

Cloud computing, or on-demand computing, provides access to shared computing resources (e.g. networks, servers, storage, applications, and services). This capacity is provided using "pay for use" models, similar to those used for traditional utilities such as water or electricity.

Cloud computing eliminates the need to buy hardware or software. This allows governments to move from a capital expense model to an operational expense model. Moreover, cloud computing is best positioned to satisfy the substantial need for agility and scalability of today's unpredictable business environments.

In the context of cloud, enterprise-wide and shared solutions, departments and agencies have a duty to apply safeguards that will enable them to retain uncompromised control over information they have collected or created.

Adopt cloud computing services

TBS will publish the Government of Canada's Cloud Adoption Strategy to guide the adoption of cloud computing services in a cost effective and secure manner. Departments and agencies will choose cloud computing services from a number of options that will include extensions to existing legacy solutions and private and public cloud offerings. In making these choices, departments and agencies will need to consider:

- Privacy
- Security
- Compliance
- Data residency and sovereignty
- Vendor lock-in considerations
- Commercial risk
- Latency and performance
- Data transfer
- Integration

Departments and agencies will consider solutions that employ Software as a Service (SaaS) before Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

To ensure Canada's sovereign control over its data, departments and agencies will adopt the policy that all sensitive or protected data under government control will be stored on servers that reside in Canada. Departments and agencies will evaluate risks based on an assessment of data sensitivity, and apply the appropriate security controls for cloud services.

Establish a cloud service broker

A cloud service broker (CSB) functions as a bridge between organizations and cloud providers. Using a CSB makes cloud services less expensive, easier, safer and more productive for organizations to navigate, integrate, consume and extend cloud services, particularly when services span multiple and diverse providers.

A CSB's key functions are procurement, billing, security accreditation, networking, credential and identity federation, application integration, customer support, and vendor service-level agreements (pertaining to management and skills).

SSC will create and operate a "light-touch" CSB role that includes all these functions, including access to SaaS, PaaS, IaaS and marketplace (online storefront) services.

Offer public cloud services

A public cloud refers to a cloud environment shared by multiple tenants that are isolated from each other. SSC will direct its efforts toward acquiring and brokering multiple enterprise-grade public cloud services. Several of these will have a presence in Canada with the capability to store and process protected data. Public cloud services will be the priority choice for departments and agencies when choosing a cloud deployment model.

Offer private cloud services

A private cloud has the attributes of a public cloud, except that the services are for use by a single enterprise, in this case the Government of Canada. The cloud's hardware, storage and networks are dedicated to a single client and typically require capital investment.

Private clouds can be implemented as pre-engineered commercial offerings or as tailored solutions engineered and assembled by staff. SSC will direct its efforts toward acquiring the former, with the latter being implemented when unique requirements arise. Departments and agencies will use private clouds where needs cannot be met by public clouds.

Information sharing

Interoperable platforms are the backbone of data and information sharing, big data analytics and collaboration. By seizing on these opportunities, government can create a modern workplace in which employees have the enabling tools needed to keep pace with the expectations of the Canadians and businesses they serve.

Build a platform for enterprise interoperability

Enterprise interoperability fosters openness and collaboration. To strengthen digital business and promote integrated business services among enterprise systems, TBS, PSPC, and SSC will create a set of modern integration tools called the GC Interoperability Platform. This platform will act as an information broker, enabling the exchange of data and information between back-office enterprise systems and organizational applications.

The platform will feature a service bus and a message fabric, built and operated by PSPC and SSC. The service bus will connect enterprise applications for integrated business needs and

the message fabric provides the messaging infrastructure that connects and enables communication between components. The two features will combine to provide a dedicated, secure and high-speed information access layer, allowing organizations to easily share data.

Government application programming interfaces (GAPIs), a single language used across siloed business systems, will allow for interoperable business by using common information exchange standards. TBS will lead the creation of common and approved GAPIs from "single sources of the truth" to support information sharing within government. TBS will also establish governance for enterprise interoperability and information sharing.

Introduce a government mobile applications store

Canadians and business want to use mobile applications to interact with government data and obtain government services. TBS will lead the creation of mobile application stores that enable digital distribution of easy-to-use and trusted mobile applications.

Introduce a government API store

An application programming interface (API) is a set of routines, protocols and tools for building software applications. An API specifies how software components should interact and how APIs are to be used in programming user interfaces. APIs are increasingly becoming the way to facilitate sharing of government data and information. TBS will lead the creation of an API store to support information sharing with Canadians, business and other entities external to government.

Implement a platform for external collaboration

Technology makes it easier for citizens, academia, scientists, businesses and government to share ideas and information and to collaborate with one another. TBS will lead the establishment of an external collaboration service provider to host departments and to provide them with a dedicated workspace and computing storage for unclassified and transitory data. Cloud pilot projects will test-drive requirements and determine the most suitable platform to meet government business, information and security needs.

TBS, in collaboration with departments, agencies, PSPC and SSC, will provide departments and agencies with a secure platform to share opinions, information and analyses, and to collaborate with external partners, academia, businesses, other governments and citizens.

While meeting the government's requirements for security classification, disposition and recordkeeping, the platform will support an array of functions such as document sharing, co-authoring, tasks, meetings and discussions.

Advance analytics capabilities

Business intelligence involves creating, aggregating, analyzing and visualizing data to inform and facilitate business management and strategy. Analytics is about asking questions and refers to all the ways in which data can be broken down, compared and examined for trends. "Big data" is the technology that stores and processes data and information in datasets that are so large or complex that traditional data processing applications can't perform analysis. Big data can make available almost limitless amounts of information, improving data-driven decision-making and expanding open data initiatives.

TBS, working with departments and agencies, will lead the development of enterprise data analytics requirements. SSC, under TBS leadership and direction, will work with departments and agencies to implement an enterprise analytics platform that takes advantage of big data and market innovation to foster better analytics and promote collaboration.

SECURE *IT*

A secure and resilient enterprise infrastructure that enables the trusted delivery of programs and services

Secure *IT* focuses on safeguarding sensitive government data and ensuring the Canadians accessing online services can trust the government with their personal information. The strategic actions outlined below align with the *Communications Security Establishment's Top 10 security practices* and with industry best practices. Departments and agencies will use the CSE Top 10 to prioritize their IT security actions that will support the elimination of active cyber threats on government networks. Table 2 (below) shows the strategic actions that are currently underway, and those that represent new enterprise directions that may require additional approvals or funding to be implemented.

ACTIONS UNDERWAY	FUTURE ACTIONS
◒ Protect web transactions to and from external-facing websites	○ Secure the government's network perimeter
◒ Implement a trusted digital identity for people accessing internal government networks and systems	○ Implement endpoint security profiles
	○ Implement an enterprise approach to vulnerability and patch management
	○ Manage and control administrative privileges
	○ Implement an improved cyber authentication service
	○ Implement a secure communication services for classified information
	○ Implement enterprise data loss prevention
	○ Enable comprehensive understanding of endpoint devices
	○ Enhance awareness of enterprise cyber security threat and risk environment

Defence in depth

Canada's competitive advantage, our economic prosperity and our national security depend upon government adopting new and accessible technologies to better serve Canadians and public service employees. If not managed well, however, making information and data more open could risk exposing networks, systems, devices and data, including personal information, vulnerable to malicious or accidental breaches. This is just one reason why strengthening IT security is paramount.

○ *Secure the government's network perimeter*

Though the Internet is a game-changer for the ease with which public service employees can access and share information, it also brings considerable risk. Malicious software (malware) can be unknowingly downloaded from websites or through email and seriously compromise IT systems and disrupt government operations.

To protect the government's network, world-class monitoring services and defensive measures have been implemented at the government's network perimeter through SSC-managed gateways. The completion of network consolidation projects will ensure that all SSC

partners use these gateways. There remain, however, organizations that continue to use non-SSC networks to access the Internet.

To address risks to the network, the Government of Canada is standardizing protection and creating a secure, government-wide network perimeter. Departments and agencies that do not currently use SSC Internet services will be migrated to the SSC-managed enterprise network and will use SSC Internet services exclusively.

TBS, CSE and SSC will establish additional Trusted Interconnection Points (GC-TIPs) between the government network and external partners to provide standardized and secure connectivity with external partners, the Internet, and to act as a gateway to cloud computing services.

These actions will reduce the risk of rogue, ad hoc or unauthorized Internet connections to and from government networks. They will also enhance the government's ability to defensively monitor data entering or exiting the government perimeter, and so ensure maximum protection of government information assets.

Implement endpoint security profiles

Malicious parties frequently seek out exposed or misconfigured Internet-facing services or equipment to gain access to IT systems or information. Endpoint devices such as laptop computers, tablets and servers provide a doorway for these kinds of threats. Malware, rootkits and phishing can lead to the loss and compromise of government data, including personal information. Operating systems and applications that use default configuration settings typically include unnecessary components, services and options. These default settings are well known and easily discovered using automated tools.

In the enterprise context, weaknesses and misconfigurations in an organization's systems could be exploited and used to attack other organizations' systems. Making the government's endpoint devices more resistant to attacks is key to securing the government enterprise.

Recognizing the risk posed by misconfigured endpoint devices, SSC, in consultation with TBS and CSE, will develop endpoint device profiles. These standardized profiles will be based on security best practices, and will represent securely configured operating systems and applications. The profiles will be validated and refreshed regularly to update their security configuration. Additional security controls, such as host-based intrusion prevention and application whitelisting – a computer administrative practice used to prevent unauthorized programs from running – will be implemented to further ensure the integrity of systems and information.

Implement an enterprise approach to vulnerability and patch management

The government must ensure that vulnerabilities are identified and remediated quickly to minimize the risk of future intrusion and potential loss. TBS and SSC will implement an enterprise-wide vulnerability and patch management capability to systematically detect and remediate vulnerabilities. Departments and agencies will implement these tools and processes, meet standard timelines for remediation, and ensure quick response times for emergency or critical patch deployment.

Manage and control administrative privileges

Organizations also need to manage internal risks to the security of their IT. Privileged accounts (such as local or domain administrators and other accounts with elevated access) are

the most powerful accounts in any organization and are also the most targeted by malicious parties that wish to compromise government information.

TBS, SSC and departments and agencies will work together to minimize the misuse of any account with elevated privileges, either malicious or accidental. Tools and processes will be implemented to ensure the proper management, control and monitoring of such accounts. These will include establishing strong authentication mechanisms for all privileged accounts.

Departments and agencies will also implement measures to manage and control the life cycle of and access to privileged accounts, including:

- Audits and reviews to confirm validity of privileges
- Continuous monitoring to look for uncharacteristic behaviour

Trusted IT

Establishing identity is fundamental to most government interactions that involve exchanging information or permitting access to sensitive resources.

Protect web transactions to and from external-facing websites

As more Canadians interface electronically with the Government of Canada, the amount of sensitive information transferred to and from government websites will increase. To maintain maximum trust in these online transactions, the government must protect them.

TBS will establish an "HTTPS everywhere" standard that will require departments and agencies to use the HTTPS protocol for all external-facing websites and cloud services. This protocol, along with approved encryption algorithms, will ensure the secure transmission of data online and the delivery of secure web services.

WHAT IS GCKey?

GCKey is a standards-based authentication service provided by the Government of Canada. It provides Canadians with secure access to online information and government services and assists Canadian federal government departments in managing and controlling access to their on-line programs through standardized registration and authentication processes.

The GCKey Service issues a GCKey, which is a unique, anonymous credential that protects communications with online Government programs and services. The GCKey service can be used for those who do not have, or choose not to use, their online banking credentials with a Sign-in Partner (SecureKey Concierge).

Implement an improved cyber authentication service

Currently, Canadians and others external to the government can securely access government services online using a trusted credential. The credential (i.e., a username and password) is either issued by the Government of Canada's GCKey service or by a private sector organization that has partnered with SecureKey Technologies to enable their customers to use their online credentials (such as card numbers or user names and passwords) to access Government of Canada services.

This mandatory solution for all online government applications offered to the public is cost-effective, secure and convenient for users. Still, improvements to the existing cyber authentication service are needed to support new initiatives such as Canada's Digital Interchange. Building on the existing solution and maintaining a pan-Canadian approach, TBS and SSC will develop a renewed cyber authentication service. This service will meet current business needs yet support enhanced functionality required for future federated identity and digital service delivery initiatives.

Implement a trusted digital identity for people accessing internal government networks and systems

TBS will complete an enterprise-wide approach to internal identity, credential and access management to:

- Reduce costs
- Promote interoperability
- Improve end-user experience (by reducing the need for multiple user IDs and passwords)

Under TBS leadership, SSC will implement common internal identity and credential processes and technologies tailored to the level of assurance required for a particular business process. For example, a unique digital identity will be needed to authenticate employees, contractors, trusted guests or any other authorized users accessing internal government networks and systems.

Departments and agencies will migrate applications to this new enterprise service when their applications are upgraded as part of regular asset life cycle maintenance.

Implement a secure communication service for classified information

Shared Services Canada, under the strategic direction of the Treasury Board Secretariat and supported by Communications Security Establishment, will implement a single, common and integrated enterprise-wide secret-level network to enable classified data to be securely transmitted, stored and processed across departments and agencies.

Every day, departments and agencies create, store and process classified information. Failure to protect this information could lead to:

- National security risks
- Economic losses
- Loss of government credibility

Although several special environments allow some organizations to safely share classified information, there is no common solution available government-wide.

SSC, under the strategic direction of TBS and supported by CSE, will implement a single, common and integrated enterprise-wide secret-level network to enable classified data to be securely transmitted, stored and processed across departments and agencies. Classified voice and mobile capabilities will also be implemented for users who need to regularly discuss classified information.

Implement enterprise data loss prevention

With its responsibility for maintaining large amounts of sensitive data, the government needs to minimize the risk of unauthorized disclosure. TBS will establish a framework to support an enterprise approach to data loss prevention. Preventing the unauthorized transfer or release of sensitive information involves first identifying sensitive data. Unauthorized data flows and operations will be monitored, detected and blocked. SSC, with departments and agencies, will implement the framework.

Awareness and understanding

Understanding the assets within an IT environment is essential to knowing what to protect and enables the government to be more proactive and efficient when responding to threats and attacks.

Enable comprehensive understanding of endpoint devices

It is critical to be able to proactively and accurately determine the status of all endpoint devices, what is running on them and who is accessing them. In this way, endpoint devices that pose a risk to the enterprise can be identified, allowing the government to become more effective when responding to threats and attacks.

Under TBS leadership, SSC, and departments and agencies will acquire and implement tools and processes to enable a real-time, enterprise view of the current status and configuration of government endpoint devices. This includes information on:

- Hardware and software versions
- Operating system versions
- Patch installations

Enhance awareness of enterprise cyber threat and risk environment

Departments and agencies are accountable for managing cyber risks to their particular program areas. However, as the government adopts an enterprise approach and programs and services become more integrated, it will be imperative that cyber risks are also managed at the enterprise level.

Key to effective enterprise risk management is understanding the changing cyber-threat landscape (e.g., who is trying to exploit government networks and systems, by what means, and for what purpose).

TBS will establish a centralized capability to continuously monitor and analyze the enterprise cyber-risk landscape. This monitoring will pull together data from multiple sources, e.g. threat assessments, risk registers, investment plans, audit results, critical asset listings, etc., to feed a consolidated enterprise view of cyber risks. One of the key data sources will be the GC Enterprise Threat Assessment, which CSE will refresh on an ongoing basis to keep pace with evolving internal and external cyber-threat environments.

The continuous monitoring of the cyber-threat and -risk landscape will inform decision-making and influence how corrective actions are prioritized across the enterprise to ensure maximum protection of government assets.

MANAGE *IT*

Smart investments that are both high in value and cost-effective

Manage *IT* addresses the management and governance of IT across government in a way that ensures IT investments take advantage of economies of scale, demonstrate value and are sustainable. *Table 3* (below) shows the strategic actions that are currently underway, and those that represent new enterprise directions which may require additional approvals or funding to be implemented.

ACTIONS UNDERWAY	FUTURE ACTIONS
Establish enterprise IT governance	Document roles and responsibilities for IT and IT security
Develop methods to prioritize investments in legacy and transformation initiatives	Lead innovation
Evolve IT management practices, processes and tools	Adopt modern and flexible business models
Develop enterprise architectures for business and information	Ensure IT infrastructure sustainability
Adopt agile approaches to implementing IT solutions	Rationalize investments

Governance

To fully embrace an enterprise IT approach, departments and agencies need clear direction on agreed-upon priorities and approved approaches, which comes from an authoritative source. Oversight is required to ensure sustained progress in advancing shared objectives. Roles and responsibilities must be documented for effective implementation of an IT governance structure.

Establish enterprise IT governance

The Deputy Minister and Assistant Deputy Minister Committees on Enterprise Priorities and Planning (CEPP) will encourage departments and agencies to move toward enterprise IT solutions for consolidated services. CEPP will establish the "rules of engagement" for adopting enterprise IT solutions and services, including the process for addressing exceptions.

Adopting an enterprise approach requires sound governance structures that support clear and informed decision-making. The Deputy Minister and Assistant Deputy Minister Committees on Enterprise Priorities and Planning (CEPP) will be the governance and oversight bodies for all government IT investments.

CEPP will encourage departments and agencies to move toward enterprise IT solutions for consolidated services. CEPP will establish the "rules of engagement" for adopting enterprise IT solutions and services, including the process for addressing exceptions. As such, CEPP will approve all implementation plans for enterprise services.

CEPP will manage demand from departments and agencies for SSC IT infrastructure services, and guide how SSC provides those supply-side services. SSC will report to CEPP on its progress with transformation efforts. Through principles-based prioritization and a risk-based approach to balancing demand and supply, CEPP will align IT and IT-enabled initiatives with enterprise business priorities.

In addition, CEPP will provide direction for and oversee the implementation of the Government of Canada IT Strategic Plan. The Committees' Terms of Reference, including mandates, authorities and accountabilities, have been updated accordingly.

All the business needs of government will be managed according to IT governance principles. Under CEPP leadership, TBS will:

- Clearly define the key roles of business owner, service provider and client
- Clarify how existing governance structures will be integrated with the IT governance structure
- Determine an appropriate decision-making process
- See that departments and agencies avoid duplication or unnecessary overlap

Develop methods to prioritize investments in legacy and transformation initiatives

The Deputy Minister and Assistant Deputy Minister Committees on Enterprise Priorities and Planning (CEPP) endorses four IT investment principles which guide departmental investment strategies ensuring they reflect business and enterprise priorities.

Principle 1: Think "Enterprise" first
Principle 2: Use cloud computing services
Principle 3: Meet common business needs through shared services
Principle 4: Examine options

SSC and PSPC will develop and define methods with which to measure the progress of transformation initiatives, aligning them with key benefits. Progress must be reported clearly and reliably.

SSC, supported by TBS and departments and agencies, and under the oversight and direction of CEPP, will develop a methodology to prioritize and allocate funding for investments in legacy and transformation initiatives. SSC will also develop a clear process to address funding deficiencies. Methodologies and processes will be refined periodically to ensure accurate determination and reporting of savings. CEPP endorses a principles-based approach to guide departmental investment strategies ensuring they reflect business and enterprise priorities. New or significant changes to IT and IT-enabled projects will be subject to consultation with TBS and approval by CEPP.

Document roles and responsibilities for IT and IT security

Departments and agencies have a role in managing and delivering IT, as described in Appendix D. TBS will work to elaborate and document the roles and responsibilities of departments and agencies, SSC, PSPC and central agencies for delivering IT services and implementing the government's IT strategic plan so that they are clearly defined, communicated and executed. TBS will also continue to provide clear direction to departments and agencies on IT security roles and responsibilities. These include security-control objectives and other security-related requirements.

Practices

Sound IT management starts with consistent planning based on documented descriptions of the enterprise. With an understanding of what's in play, IT managers can adopt solutions that best address their business needs.

Evolve IT management practices, processes and tools

CIOs should plan and execute departmental IT plans in a way that aligns with the government's IT strategic plan and overall enterprise modernization priorities. Important tools to support them include:

- Investment plans
- Architectural reviews
- Application Portfolio Management
- Expenditure Reporting
- Performance Reporting

Optimizing IT investments to meet business outcomes will propel the evolution of IT management processes and tools. TBS policy and guidance will allow departments and agencies to:

- Manage IT consistently and with greater maturity

- Better understand IT at the enterprise level
- Benchmark themselves against similar organizations
- Monitor and track progress against government priorities
- Set future priorities

TBS will also provide policy guidance to assist departments and agencies:

- Develop sound project cost estimates
- Implement good project management practices in the area of complex IT projects

Develop enterprise architectures for business and information

Describing the enterprise allows us to understand how government processes work. Enterprise architectures show where there are similarities and differences in business units, programs and departmental boundaries.

IT enterprise architectures show:

- What IT systems are in use
- How IT systems interact
- How mission-critical business applications are deployed across the government's IT infrastructure

Understanding enterprise architecture enables effective decision-making about IT investments, costs and risks. It allows us to optimize performance and deliver on government priorities in the digital era.

Working with functional communities, TBS will lead the development of an enterprise architecture framework.

Adopt agile approaches to implementing IT solutions

Departments and agencies will take advantage of existing multi-departmental contracts when investing in solutions to meet common needs. In cases where multi-departmental contracts or tools do not meet identified business requirements, departments and agencies will contact TBS to discuss other options. Departments and agencies are required to keep TBS up to date on their investments and plans.

Where a customized or in-house solution is the only choice, application development teams should adopt modern agile approaches that deliver greater speed and agility. They must also take into account the increasingly complex IT ecosystem of interdependent software architecture, infrastructure and processes.

Departments and agencies will promote a learning culture that allows IT solutions architects and developers to:

- Understand and adopt iterative development approaches, automate release schedules and embrace a layered testing strategy, including automated testing
- Increase engagement with business colleagues to advance iterative approaches
- Adopt an approach that considers a service-oriented architecture (SOA) and application programming interface (API) first, rather than monolithic constructs

Innovation

The Government of Canada is transforming its IT to better serve Canadians, with innovation key to delivering on this agenda. Successful innovation combines creativity with process to transform novel ideas into business enablers that deliver tangible results. It embraces experimentation and intelligent risk taking, bringing new approaches which address existing problems and leverage future opportunities. Innovation calls for collaboration both with new and traditional partners, identifying and breaking down any barriers that prevent us from achieving maximum results.

Lead innovation

The role of CIOs is evolving from service provider to full strategic business partner. These leaders are innovation agents, business enablers, and catalysts for enterprise transformation. Departmental CIOs will be strategic business partners who bring IT innovations to the table to address the organization's business needs.

Adopt modern and flexible business models

To achieve a better balance between demand and capacity, SSC and PSPC will fully adopt cost-recovery business models for all IT services. As an enterprise, departments and agencies will achieve better business value by sharing IT resources, capacity and capabilities.

Sustainability

Ensuring that IT investments are sustainable and meet business needs will enable departments and agencies to deliver better services to Canadians.

Ensure IT infrastructure sustainability

A sustainable funding model must take into account the regular renewal cycle of IT infrastructure assets with the appropriate level of investment. TBS and SSC will explore alternative financial models to address IT renewal.

Rationalize investments

In keeping with CEPP investment principles, spending on new or significant changes to certain IT and IT-enabled projects will be subject to consultation with TBS and approval by CEPP. This includes spending on systems for common business domains such as:

- Case management
- Information management
- Human resources management
- Financial management
- Other back office administrative processes
- Identity and credential solutions
- IT infrastructure and associated solutions

Departments and agencies will take an enterprise approach to managing their portfolio of applications to determine opportunities for common, government-wide solutions, as well as retire aging and at-risk applications. Those applications that remain in use, supporting mission-critical business functions, are to be kept evergreen until they can be replaced by modern solutions.

WORK *IT*

An agile, connected and high-performing workforce with modern tools

Work *IT* is focused on building a high performing IT workforce and ensuring that public service employees have a modern workplace and the IT tools they need to do their jobs. *Table 4* (below) shows the strategic actions that are currently underway, and those that represent new enterprise directions which may require additional approvals or funding to be implemented.

ACTIONS UNDERWAY	FUTURE ACTIONS
Invest in executive talent management	Promote gender parity
Enhance workforce planning	Promote digital literacy and collaboration
Enable career development	
Modernize workplace technology devices	
Support a mobile workforce	
Provide Wi-Fi access	
Provide desktop videoconferencing to employees	
Implement managed print services	
Advance digital collaboration	

IT workforce

Successfully delivering IT services requires a skilled, agile, connected and high-performing IT workforce that combines a knowledge of business and technology. IT professionals need to be able to keep pace with the speed at which technology is evolving. To enable a high-performing, strategic IT workforce will require continued investment in career and talent management.

Invest in executive talent management

Talent management reviews and succession planning identify key skills gaps and mitigation strategies for the enterprise as a whole. Such efforts are supported by the 2016 Management Accountability Framework, which includes talent management indicators for CIOs and IT assistant deputy ministers.

Departments and agencies will support enterprise-wide IT executive talent management and succession planning by:

- Identifying sources of new talent to address gaps
- Identifying and creating opportunities at various levels
- Promoting and fostering the leadership and strategic partner component of the new and emerging CIO role
- Encouraging and facilitating learning and assignment opportunities for CIOs and aspiring CIOs
- Encouraging CIOs to explore diversified career paths, both within and outside IT organizations

Enhance workforce planning

Building on efforts to better understand the workforce in the IT community, departments are developing three-year departmental workforce strategies. These strategies will serve as a foundation for workforce planning. To support successful business outcomes, they will align

with the departments' human resources plans and the government's enterprise approach for IT.
TBS will leverage this work in order to provide enterprise-level analysis that will identify:

- Shifts and gaps in workforce complement and competencies
- Emerging issues
- Strategic opportunities

TBS will work with departments and agencies to explore new approaches to utilize internal capacity to meet current and future needs.

TBS will continue to evolve tools to support workforce planning and to project workforce requirements in the future. One such example is IT Community Generics, a suite of tools to help CIOs and IT managers direct IT resources in a way that reflects best practices in IT organizational design. IT Community Generics facilitate an enterprise approach to managing IT human resources.

Enable career development

IT professionals need to be well positioned to support CIOs in their evolving role as strategic business enablers and partners. Competency tools, available through IT Community Generics, support computer science (CS) career development. Career-development materials, including career-related research on GCpedia, will further enable IT professionals to identify career paths and required competencies.

TBS will lead the development of an internal skills inventory of the public service IT workforce and make it available to departments and agencies.

Working with government and private sector stakeholders, including industry associations, TBS will share best practices, identify trends and support IT career development. The Canada School Public Service will design new learning products that target new and non-traditional skills for IT professionals.

Promote gender parity

An innovative workplace demands a workforce that accurately represents the full breadth of the Canadian talent pool. Currently, IT remains predominantly a male domain. Recent data reveals that women occupy only 27% of all CS positions in the Government of Canada. What's more, the percentage of women in younger cohorts has diminished steadily to a low of 13% in the under-30 age group.

To support the government's commitments to gender parity and a balanced and diverse workforce, departments and agencies will develop and leverage partnerships with organizations that encourage IT as a career choice for young women. TBS will work with these organizations and with post-secondary institutions to ensure that women in IT programs, as well as potential candidates, are aware of job opportunities in the field. Departments and central agencies will also work to increase labour mobility among women by encouraging leaders from within the public service, as well as the private sector, to consider roles within the government's CIO community.

To retain women within the IT community, departments and agencies will encourage developmental opportunities such as internships and mentorships. TBS will develop communications to raise awareness of opportunities for women to develop, advance and participate fully in the IT workforce.

Initiatives such as the Women in Communications and Technology Public Sector Network, a government-wide forum designed to engage women in IT, provide opportunities for women to network and take advantage of professional development programs.

Modern workplace

Technology is a key enabler of a modern workplace that supports collaboration, innovation and mobility. Ensuring that smart technology provides a consistent, accessible workplace experience throughout government will improve how all employees work together and deliver better services to Canadians.

Modernize workplace technology devices

Workplace technology devices are essential for a modern workplace and a collaborative, mobile workforce, consistent with the Blueprint 2020 vision. TBS will work closely with departments and agencies to ensure that workplace technology devices meet the Blueprint 2020 vision.

TBS will establish enterprise standards and processes for life cycle management and set direction to guide future workplace technology devices standards and configurations.

SSC will continue to consolidate contracts and procurement activities to improve security, reduce costs and improve service to Canadians. SSC will procure workplace technology devices, and work with TBS, and departments and agencies to standardize devices.

Departments and agencies are responsible for support and maintenance of workplace technology devices. They will explore support models such as self-service and regional clusters, to reduce costs while promoting consistent user experience and service expectations.

Support a mobile workforce

The Government of Canada is committed to and encourages an open and collaborative work environment where mobile devices are used. Departments and agencies will balance the cost of these devices, and their support, against the business value achieved.

Provide Wi-Fi access

Access to wireless data networks is critical for employee productivity. The broader deployment of Wi-Fi may also reduce costs by displacing the need to provide wireline infrastructure, which is expensive to install and maintain.

TBS and SSC will put in place the necessary services and policies to support Wi-Fi usage. Departments and agencies will implement Wi-Fi access to data networks for all employees within common areas and their workspaces, where the job requires mobility. Departments and agencies will migrate to Wi-Fi-capable devices and support Wi-Fi access to local area networks for registered users, as well as Wi-Fi guest-network access where security requirements are appropriate.

Provide desktop videoconferencing to employees

Increased access to videoconferencing supports the collaborative operations of virtual teams across organizations, time zones and regions. Departments and agencies will complete the re-engineering of their in-house videoconferencing facilities to enable full interconnectivity across the government. Where appropriate, and where the user profile supports such functionality, SSC will also create the network and bandwidth capacity needed to support videoconferencing at desktops.

Implement managed print services

The Government of Canada will continue to improve the sustainability of workplace operations by completing the implementation of the Office of Greening Government Operations' strategy for printing. Departments and agencies will achieve an 8:1 average ratio of office employees to printing units. Departments and agencies will also use SSC's managed print services to facilitate improvements to their organizations' environmental efficiencies in imaging, specifically, reduced energy costs and paper consumption and proper disposal of electronic equipment.

Digital collaboration tools

Digital collaboration refers to the skills and mindset needed to work effectively in an open digital environment. Tools that respect government requirements such as accessibility, privacy, security, information management and official languages will be used to promote digital collaboration.

Promote digital literacy and collaboration

Digital literacy goes beyond basic computer skills. And it's essential to make the most of investments already made in IT infrastructure, devices and tools and to ensure that IT helps workforce productivity rather than detracts from it.

Public service employees should be able to use GCTools such as GCpedia, GCconnex and GCintranet channels to share information and to build the professional networks needed to respond to shifting priorities and problems. Collaborating digitally involves "working out loud," where others can see, benefit from and help improve how employees work.

To promote a culture of openness and collaboration, departments and agencies will nurture these skills throughout public service by:

- Adopting and using GCTools for everyday work
- Deploying targeted and general learning and community outreach activities
- Promoting the use of self-directed learning tools and materials

Senior leaders' adoption of GCTools will be critical to successfully integrating digital collaboration into their organizations and to demonstrating the full benefits of these collaborative tools. Leaders will adopt an "open first" attitude toward content creation and encourage their employees to participate in shared-knowledge and collaborative digital spaces, other than where security requirements prohibit this.

Advance digital collaboration

GCTools such as GCpedia, GCconnex and the GCintranet channels enable collaboration across the government. Employees are able to access and share information and work across departments, agencies and geographic boundaries, resulting in better service to Canadians.

GCTools that support government requirements on accessibility and official languages will be further developed and integrated into other applications. This will allow employees to easily connect with the colleagues and information they need to work effectively. GCTools will connect to a digital workspace that provides simplified access to other activities such as staffing, learning and professional development.

TBS will make adopting GCTools part of standard practices for employee onboarding throughout government. Departments will then be in a better position to adopt and use GCTools through the Ambassadors Network and in formal training and ongoing communications. The Ambassadors Network consists of volunteers from various departments

The Ambassadors Network consists of volunteers from various departments and regions that provide support to teams on the use of GCpedia and GCconnex.

or regions that provide support to teams on the use of GCpedia and GCconnex to enhance their work.

Departments and agencies will decommission standalone collaborative platforms unless they are linked to core local business requirements. Email communication will be reduced in favour of open discussions or in favour of instant messaging, where transitory communications can occur without bogging down government systems.

The Way Forward

Implementing the plan

In support of the Government of Canada, the Deputy Minister Committee on Enterprise Priorities and Planning (CEPP) will provide oversight and guidance on government IT investments, supported by the Assistant Deputy Minister (ADM) CEPP. An implementation roadmap for the plan's initiatives has been developed (Appendix A) and financial analysis is underway to help determine the extent and pace of implementation, particularly in terms of infrastructure modernization. This roadmap will be refined as planning advances.

Guided by CEPP, TBS will work with SSC, PSPC and departments and agencies to prioritize the elements of the plan and, as these initiatives are more fully developed, approved and funded, to implement them. Not all actions set out in this plan will be completed by 2020 and some actions may not be appropriate for all organizations, most notably small departments and agencies. Deputy heads, in consultation with TBS, will take this into consideration when preparing their own IT strategies.

Risks and mitigation strategies

The following risks to implementation and their mitigation strategies are identified:

Lack of capacity (people): There is a risk that the government will not have sufficient capacity to implement the plan. **Mitigation:** Some strategic actions are identified as directional and can be deferred until sufficient capacity is available. CEPP (governance) will provide direction and oversee the implementation of the plan.

Too much to do: There is a risk that the plan is overly ambitious and that the government will not be able to absorb all the new work. **Mitigation:** Some strategic actions are identified as directional and can be deferred until sufficient capacity is available. CEPP (governance) will provide direction and oversee the implementation of the plan.

Insufficient funds: There is a risk of insufficient funding to implement all strategic actions identified in the plan. **Mitigation:** Strategic actions that are identified as directional will not proceed until funding is secured. Those currently underway will be assessed to ensure sufficient funding is available to complete implementation.

Failure to adopt the enterprise approach: There is a risk that departments and agencies will not all act in an enterprise manner. **Mitigation:** CEPP will encourage departments and agencies to move toward enterprise IT solutions for consolidated services and address exceptions.

Retiring IT workforce/skills gaps: There is a risk that the government will not retain its IT workforce due to increasing retirements and gaps in required skills. **Mitigations:** impacts

could be avoided by actions to enhance workforce planning, enable career development, promote gender parity, and invest in executive talent management.

Significant cyber event: There is a risk that a significant cyber security event could occur, delaying implementation of the plan. **Mitigation:** the impact of such an event could be reduced through measures such as securing the network perimeter, implementing security profiles for endpoint devices to reduce malicious threats, implementing vulnerability and patch management, and enhancing enterprise-wide awareness of the government's cyber threat and risk environment.

Measuring progress

CEPP will provide direction and oversight of the implementation of the Government of Canada IT Strategic Plan including the monitoring of enterprise-wide implementation risk.

Progress towards achieving the strategic goals outlined in the IT strategic plan will be tracked, evaluated and reported. Key performance indicators (KPIs) have been identified for strategic actions and are shown in Appendix B. The indicators will be reviewed in 2016 and revised as required. Benchmarks and targets will also be established in 2016, in consultation with departments and agencies, and leveraging existing assessment frameworks and tools, such as the Management Accountability Framework, key performance indicators for internal services, and departmental priorities and performance reports.

CEPP will track the overall progress of the strategic plan and a yearly progress report will be provided to the Secretary of the Treasury Board.

Staying evergreen

On an ongoing basis, CEPP will assess progress, consider the strategic plan's effectiveness and align resources with priorities to get the intended results. The plan will also be kept evergreen through annual reviews. The first update to the plan is scheduled for June 2017. Going forward, updates will be aligned to the annual departmental IT planning cycle and completed in September to allow departmental IT plans to reflect new directions.

Advised by CEPP, TBS will make adjustments where necessary to ensure that the strategic direction:

- Remains relevant and aligned with government priorities
- Addresses IT issues
- Keeps pace with the ever-changing technology landscape
- Assigns appropriate accountabilities

By ensuring a strategic, whole-of-government approach to the Government of Canada's information technology investments, we will drive better service to Canadians, ensure our networks and information are more secure, and deliver better value for money. We will enable the public service to deliver its best for Canadians.

Appendix A: Implementation Roadmap

		Strategic Actions	Status		Involved	Target Completion Date
			Underway[1]	Directional		
Service IT		**Service Management and Modernization**				
	1	Develop IT service portfolios and catalogues	•		SSC, PSPC	2017
	2	Report on key areas of IT system health performance	•		SSC, PSPC	2017
	3	Implement enterprise IT service management tools		•	SSC, Departments	
	4	Complete data centre consolidation and modernization	•		SSC, Departments	2020
	5	Complete network consolidation	•		SSC, Departments	2020
	6	Complete government email consolidation	•		SSC, Departments	2020
		Cloud Computing				
	7	Adopt cloud computing services	•		TBS, SSC, Departments	
	8	Establish a cloud service broker	•		SSC	
	9	Offer public cloud services	•		SSC	
	10	Offer private cloud services		•	SSC	
		Information Sharing				
	11	Build a platform for enterprise interoperability	•		TBS, PSPC, SSC	2019
	12	Introduce a government mobile applications store		•	TBS	
	13	Introduce a government API store		•	TBS	
	14	Implement a platform for external collaboration		•	TBS	
	15	Advance analytics capabilities		•	SSC, Departments	
Secure IT		**Defence in Depth**				
	16	Secure the government's network perimeter		•	TBS, SSC	
	17	Implement endpoint security profiles		•	TBS, SSC, CSE, Departments	
	18	Implement an enterprise approach to vulnerability and patch management		•	TBS, SSC, Departments	
	19	Manage and control administrative privileges		•	TBS, SSC, Departments	
		Trusted IT				
	20	Protect web transactions to and from external-facing websites	•		TBS, SSC, Departments	2018
	21	Implement an improved cyber authentication service		•	TBS, SSC	
	22	Implement a trusted digital identity for people accessing internal government networks and systems	•		TBS, SSC, Departments	2018
	23	Implement a secure communication service for classified information		•	TBS, CSE, SSC, Departments	
	24	Implement enterprise data loss prevention		•	TBS, SSC, Departments	
		Awareness and Understanding				
	25	Enable comprehensive understanding of endpoint devices		•	TBS, SSC, Departments	
	26	Enhance awareness of enterprise cyber security threat and risk environment		•	TBS, CSE, Departments	

[1] Project details, (e,g, plans, milestone dates, performance measures) can be found in departmental plans.

Implementation Roadmap

	Strategic Actions		Status		Involved	Target Completion Date
			Underway[2]	Directional		
Manage *IT*	**Governance**					
	27	Establish enterprise IT governance	•		TBS	2017
	28	Develop methods to prioritize investments in legacy and transformation initiatives	•		SSC	2017
	29	Document roles and responsibilities for IT and IT security		•	TBS	2017
	Practices					
	30	Evolve IT management practices, processes and tools	•		TBS, Departments	On-going
	31	Develop enterprise architectures for business and information	•		TBS, Functional communities	On-going
	32	Adopt agile approaches to implementing IT solutions	•		Departments	On-going
	Innovation					
	33	Lead innovation		•	Departments	
	34	Adopt modern and flexible business models		•	SSC, PSPC	
	Sustainability					
	35	Ensure IT infrastructure sustainability		•	SSC	
	36	Rationalize investments		•	TBS, SSC, Departments	
Work *IT*	**IT Workforce**					
	37	Invest in executive talent management	•		TBS, Departments	On-going
	38	Enhance workforce planning	•		TBS, Departments	On-going
	39	Enable career development	•		TBS, Departments, CSPS	On-going
	40	Promote gender parity		•	TBS, Departments	
	Modern Workplace					
	41	Modernize workplace technology devices	•		TBS, SSC, Departments	On-going
	42	Support a mobile workforce	•		SSC, Departments	2020
	43	Provide Wi-Fi access	•		TBS, SSC, Departments	2020
	44	Provide desktop videoconferencing to employees	•		SSC, Departments	2020
	45	Implement managed print services	•		SSC, Departments	On-going
	Digital Collaboration Tools					
	46	Promote digital literacy and collaboration		•	TBS, Departments	
	47	Advance digital collaboration	•		TBS, Departments	On-going
	Modernization Priorities (Refer to Appendix C)					
	HR Transformation (My GCHR)		•		TBS-OCHRO	2019
	IM Transformation (GCDocs)		•		TBS-CIOB	2019
	Financial Management Transformation		•		TBS-OCG	2018
	Shared Case Management		•		TBS-CIOB	2016
	Canada.ca (web renewal)		•		TBS-CIOB	2018
	Government identity, credential and access management service (ICAM)		•		TBS-CIOB, SSC	2021

[2] Project details, (e,g, plans, milestone dates, performance measures) can be found in departmental plans.

Appendix B: Key Performance Indicators

	Strategic Actions	Key Performance Indicators
Service *IT*	1. Develop IT service portfolios and catalogues	Published catalogues Client satisfaction with service targets Time lag to resolve a service target issue
	2. Report on key areas of IT system health performance	Client satisfaction
	3. Implement enterprise IT service management (ITSM) tools	Number of departments and agencies using enterprise ITSM tools
	4. Complete data centre consolidation and modernization	Number of data centres
	5. Complete network consolidation	Number of departmental wide-area networks
	6. Complete government email consolidation	Number of departmental email systems
	7. Adopt cloud computing services	Percentage of operational spending allocated to cloud computing services
	8. Establish a cloud service broker	Client satisfaction
	9. Offer public cloud services	Percentage of operational spending allocated to public cloud computing services
	10. Offer private cloud services	Percentage of operational spending allocated to private cloud computing services
	11. Build a platform for enterprise interoperability	Number of departments/departmental systems connected to the interoperability platform
	12. Introduce a government mobile applications store	Client satisfaction
	13. Introduce a government API store	Client satisfaction
	14. Implement a platform for external collaboration	Client satisfaction
	15. Advance analytics capabilities	Service use
Secure *IT*	16. Secure the government's network perimeter	Percentage of departments and agencies migrated to SSC-managed gateways Percentage of external partners using GC trusted interconnection points
	17. Implement endpoint security profiles	Percentage of devices using SSC standardized endpoint device profiles Percentage decrease in the impact of security breaches and incidents
	18. Implement an enterprise approach to vulnerability and patch management	Time to deploy patches (response time) Percentage of systems with critical vulnerabilities
	19. Manage and control administrative privileges	Number of privileged accounts (reduction) Percentage of privileged accounts configured for strong authentication
	20. Protect web transactions to and from external-facing websites	Rate of compliance to standard
	21. Implement an improved cyber authentication service	Number of new initiatives supported by the governments cyber authentication service (Adoption rate) Client satisfaction
	22. Implement a trusted digital identity for people accessing internal government networks and systems	Number of applications using the GC internal credential authentication service
	23. Implement a secure communication service for classified information	Number of departments and agencies using the common enterprise-wide secret network service
	24. Implement enterprise data loss prevention	Number of incidents (involving unauthorized disclosure of sensitive data)
	25. Enable comprehensive understanding of endpoint devices	Reduced time to investigate security incidents
	26. Enhance awareness of enterprise cyber security threat and risk environment	Number of systems monitored within the enterprise dashboard

	Strategic Actions	Key Performance Indicators
Manage *IT*	27. Establish enterprise IT governance	Rules of engagement established Percentage of departments adopting enterprise solutions
	28. Develop methods to prioritize investments in legacy and transformation initiatives	Documented methodology Number of IT and IT-enabled projects approved by CEPP
	29. Document roles and responsibilities for IT and IT security	Employee awareness of roles and responsibilities Number of employees trained in IT and IT Security awareness
	30. Evolve IT management practices, processes and tools	Percentage of variance between budgets, forecasts and actual costs
	31. Develop enterprise architectures for business and information	Percentage of IT budget assigned to enterprise architecture development and maintenance
	32. Adopt agile approaches to implementing IT solutions	Number of multi-departmental contacts being used Average time to deliver functionality, based on measures such as function point or modules
	33. Lead innovation	Percentage of IT budgets assigned to innovation
	34. Adopt modern and flexible business models	Cost-recovery business models adopted Number of departmental IT plans with full costing (including SSC component)
	35. Ensure IT infrastructure sustainability	Sustainable funding model in place
	36. Rationalize investments	Number of at-risk applications retired Application evergreen plans in place Number of projects aimed at implementing common enterprise solutions
Work *IT*	37. Invest in executive talent management	Percentage of organizations that have a succession plan in place for the CIO position
	38. Enhance workforce planning	Percentage of departments whose HR planning component in their Departmental IT Plan submissions meet the HR planning criteria requirements
	39. Enable career development	Percent of core public administration CS's with learning plans Number of departments using IT community generics (CIO Suite)
	40. Promote gender parity	Number of women occupying positions in the CS occupational group (comparison over time) Percentage of departments that have a strategy to promote gender parity
	41. Modernize workplace technology devices	Compliance to standards Mean time to resolution (help desk measurement)
	42. Support a mobile workforce	Employee satisfaction
	43. Provide Wi-Fi access	Employee satisfaction
	44. Provide desktop videoconferencing to employees	Employee satisfaction
	45. Implement managed print services	Number of departments at 8:1 average ratio of office employees to printing units
	46. Promote digital literacy and collaboration	Number of GCTools Ambassadors by department Number of GCTools information sessions offered and the number of participants per session
	47. Advance digital collaboration	Percentage of Public Servants registered on the GCTools

Appendix C: Government of Canada Modernization Priorities 2016–19

Priority	Overview
Data centre consolidation	SSC is in the process of establishing the Government of Canada's future IT infrastructure: a cost-effective and robust IT backbone that will support the current and future needs of our partner departments. As we transform our infrastructure, SSC and partner departments will need to work together to migrate applications and workloads from the legacy environment to a new, modern and consolidated environment. *Source: Workload Migration*
Network consolidation	The GCNet WAN project will consolidate and modernize Wide Area Network services for Shared Services Canada (SSC) and its Partners / Clients to reduce costs, increase security, and enhance program delivery to Canadian citizens and businesses. *Source: CIOC GCConnex (September 2014 update)*
Migration to common E-mail solution	The Email Transformation Initiative will consolidate and modernize email services to reduce costs, increase security and enhance program delivery to Canadian citizens and businesses. *Source: ETI*
Preparation for Workplace Technology Device transformation	TBS-CIOB will establish, publish and update a standard minimum software configuration for personal computers. The minimum standard will be based on an X86-64 bit and will include a minimum operating system configuration plus other software considered necessary for productivity, remote management and cyber security. *Source: GCPedia page for WTD*
Adoption of managed GC HR system	My GCHR (PeopleSoft) v9.1 has been designated as the standard for the Government of Canada people management system. My GCHR will be the one-stop solution for all HR administrative transactions. *Source: MYGCHR GCPedia page*
Adoption of GCDocs for document management	GCDOCS is the Government of Canada (GC) official Electronics Document Records Management (EDRM) solution to support organizations in their information management (IM) obligations for information lifecycle management. Within a GCDOCS enterprise repository, organizations can collect, store, share, organize, manage and search content. GCDOCS enables document centric collaboration while offering robust access controls through user and group administration rights. *Source: GCDOCS*
Shared Case Management	The goal of this initiative is to provide a common Case Management Solution to departments and agencies across the Government of Canada (GC). This is a key initiative aligned with GC IT modernization strategies. *Source: SCMS GCConnex*
GC Interoperability	The need for interoperability arises from the GC's pursuit of achieving improvements in the management and cost of government operations and for a more transparent, accountable and responsive federal government. Expected outcomes resulting from improved interoperability include Seamless information flow across jurisdictions; Cost optimizations through reuse; Increased responsiveness and agility; and Improved Reporting. *Source: GC Interoperability*
Migration of GC Web sites to Canada.ca	The Web Renewal initiative is a multi-year project that aims to enhance the effectiveness and usability of Government of Canada (GC) websites, with Service Canada functioning as the Principal Publisher for Canada.ca. Ultimately, Canada.ca will serve as a single integrated point of entry into the GC Web presence. *Source: Web Renewal*
Migration to GC Identity, Credential and Access Management Service	GC ICAM is a critical, foundational element of the overall GC Enterprise Security Architecture (ESA) Program. GC ICAM will provide a GC-wide solution that will decrease costs, enhance the experience and efficiency of end users, improve the overall security posture of GC networks, systems and applications, and provide greater control of privacy. GC ICAM will be implemented in a phased, incremental approach over a number of years. *Source: ICAM*

Appendix D: Roles and Responsibilities

The Government of Canada is made up of over 100 separate organizations that deliver a broad range of programs and services to individuals and businesses in Canada and abroad. Its programs and services are categorized into four spending areas: Economic Affairs, Social Affairs, International Affairs, and Government Affairs. IT supports the government in delivering these external-facing programs and services.

The Secretary of the Treasury Board sets government-wide strategic direction for IT, with input from organization deputy heads, chief information officers (CIOs) and other stakeholders. The responsibility for delivering IT services is shared between government organizations and central IT service providers such as Shared Services Canada (SSC) and Public Services and Procurement Canada (PSPC).

Shared Services Canada has the mandate to provide data centres, networks and email services to the largest government departments. Smaller government organizations receive these services on an optional basis. SSC, the Communications Security Establishment (CSE) and Public Safety Canada have a shared responsibility for cyber and IT security, with oversight provided by TBS. In addition, SSC is responsible for procuring hardware and software, including security software for workplace technology devices – the authorized physical devices and related software used in government office work. Departments and agencies are responsible for workplace technology device deployment, support and asset life cycle management. SSC spends $2 billion annually on the services it provides, portions of which it cost-recovers from federal organizations.

Public Services and Procurement Canada provides IT services supporting back office services such as human resource management systems, pay and pension, enterprise records and document management, and financial systems and services. SSC and PSPC jointly support federal organizations in procuring IT goods and services.

Treasury Board Secretariat, supported by the Chief Information Officer Branch (CIOB), develops strategy and sets government-wide policy and mandatory requirements for IT and cyber security, and provides guidance on implementing the direction through policy implementation notices.

Shared Services Canada's Cyber and Information Technology Security Branch
Responsibility Assignment Matrix - Explanatory Note

Overview

The Cyber and Information Technology Security Branch (CITS) of Shared Services Canada (SSC) has developed a responsibility assignment matrix, also referred to as a RACI, to map the roles and responsibilities for all security stakeholders within SSC as well as the interdependencies with SSC's partner organizations.

Development Approach

The Security Management Directorate developed the RACI for CITS beginning with internal branch consultation then solicited feedback from all stakeholders within the cyber and information technology security community, including partner organizations. Feedback from these consultations has been incorporated into the matrix.

General Principles

- The matrix is considered a living document that evolves with organizational needs and business changes. Upon approval, it is circulated and considered to be under continuous improvement without subsequent need for re-approval. Change control applied to ensure all affected stakeholders are in agreement.
- The accountable group for any given activity or process, has responsibility within that process, and must ensure that the other roles are appropriately assigned.

Business Outcomes

The CITS RACI matrix:

- was developed for clear delineation of responsibilities between SSC and its partner organizations and, in particular, to assist the Security Tripartite of SSC, Communications Security Establishment of Canada and the Treasury Board of Canada Secretariat in delineating roles and responsibilities between the lead agencies;
- deliniates responsibilities internally between authorities within SSC and those responsible for undertaking the activities; and
- distributes accountabilities between the different CITS directorates.

Shared Services Canada's Cyber and Information Technology Security Branch
Responsibility Assignment Matrix - Explanatory Note

Definitions:

Responsible (R)

- This stakeholder is consulted and informed.
- A stakeholder who is responsible to contribute work in order to achieve success on the task or function. There can be multiple Rs for a given action. They follow the direction of the accountable lead.

Accountable (A)

- This stakeholder is also considered to be responsible, consulted and informed.
- This stakeholder is the primary lead who will ensure that a take or function will be completed and can also be responsible for some of the work. An R is not added beside the A in the matrix as it is understood that this person holds both roles. There should never be more than one A on any given row unless a delineation of accountable persons is explained.

Consulted (C)

- This stakeholder must be consulted before a decision is made and must also be informed on all decisions.

Informed (I)

- This stakeholder is informed after a decision is made.

SSC Cyber and IT Security RACI

RACI Definitions

R	Responsible	Responsible to do the work or part of it, (multiple R's may be assigned per task)
A	Accountable	Makes the final decision and has the ultimate ownership ... also does some work (only one A assigned per task)
C	Consulted	Must be consulted before a decision or action is taken ... (multiple C's may be assigned per task)
I	Informed	The person who must be informed that a decision or action has been taken

Version : 16w14.2

2016-04-05

R:\ITSB\CITS\02 Management\080 CITS Organizational Development\Organization and RACI

Request changes to:

SSC.citspeerreview-cstipeerreview.SPC@canada.ca

Sensitivity: Protected A

Internal / External / Hide : 0 - Header / T -tbd / f-future /	Ref Line # (Gaps due to internal Funct. not listed)	Function	Function / Task Description	C 1 SSC-Department (Highest Level)	C 1 SSC-CITS Branch (High Level)	C 2 DG Security Management (Dinesh Mohan)	C 3 DG Cyber & IT Security Operations (Eric Belzile)	C 4 DG Infrastructure (Donald Messier)	C 5 Sr Dir. Identity & Access Management (Simon Levesque)	C 6 DG Secret Infrastructure (Dinesh Mohan)	C 7 Sr. Dir. PM (*Lucy Levesque... tbd*)	C 8 External to CITS but within SSC	C 9 Service Management & Data Centres Branch (A/Patrice Rondeau)	C 10 Networks & End User Branch (Pankaj Sehgal)	C 11 Strategy Branch (Peter Bruce)	C 12 SSC Corporate DSO (A/Marc Contois)	C 13 Corporate Services Branch (A/Elizabeth Thrompt)	C 14 (External to (SSC) Partner Department,	C 15 Communications Security Establishment (CSE)	C 16 Public Safety (PS)	C 17 Royal Canadian Mounted Police (RCMP)	C 18 Treasury Board Secretariat (TBS) Chief Information Officer Branch (CIOB)	C 19 Other (See Notes)	C 20	C 21 Notes-External	C 22 Notes-2
0	1	**1.0 IT Security Governance**																									
0	2	**1.1 Governance Board & Committee support**																									
I	3	Support Internal Governance Organizations Management (security) (e.g. SRMB)	Define security governance structure (Boards, Committees, Working Groups), Stakeholders, Partners, Lead Agencies, Mandates, Terms of Reference, Membership, Roles and Responsibilities, Consultation, Decisions and Approval Processes, Interfaces with external organizations. Leverage existing governance structures and processes. Cyber Security Strategy briefing notes, ad-hoc tasking at President and COO level.	A	A	A	R	I	I	C	I		I	I	C	I	I		I	I	C		C			DG SM is accountable. Policy & Compliance division within SM are responsible, other SM divisions are consulted. As an example, P&C division acts as secretariat for the Security Risk Management Board. TBS, CSE, DG Secret Infrastructure and PS are consulted on Cyber and IT security matters; Strategy Branch - Strategic Policy, Planning and Reporting as well as Analytics , Benchmarking and Transformation Program are consulted.
I	4	Change Advisory Boards (CAB)	This functions involves CITS/SM support to the Change Advisory Board(s) to ensure that the changes within the mandated SSC IT infrastructure (End-state and Legacy) do not adversely impact the security posture of SSC system and services. CITS/SM activities focus on engaging CITS Subject Matter Expertise to ensure that changes do not adversely impact: - overall compliance with the GC security policy instruments; - the status of ATO and ATO conditions; and - system residual risks based on vulnerability, categorization and threat environment.	R	R	R	R	R	R	R	R		A	C											
E	5	Security Tripartite Boards and Committees a) Enterprise Security Architecture (ESA) b) Government of Canada Security Council (GCSC) c) DG Cyber	Tripartite membership: Treasury Board Secretariat (TBS/CIOB), SSC, and Communications Security Establishment (CSE). Active participation to: Ensure coordinated development of the GC-wide enterprise security architecture for implementing IT security across the GC in alignment with SSC initiatives; Align cyber security strategic priorities with the enterprise direction established by ADM and DM-level tripartite committees; Ensure that horizontal cyber security initiatives are aligned with Enterprise strategic priorities; and Ensure monitoring and oversight to achieve timely implementation; GCSC: Ensure the development, implementation and ongoing evaluation of an integrated Government of Canada Security program to support GC Security objectives.	R	R	R	R	I	I	I					I				I	R	A*	I	A*		A* Certain functions are accountable (no overlap) Rs for CITS indicate responsibility to participate in committee work and decision making. Assignments are intended to reflect participation in Security Tripartite (TBS/CSE/SSC) committees. Other GC committees such as GCSC may require Partner consultation.	DG Security Management is Responsible working with TBS for this function. Security Operations is responsible for GCSC. Representative of the tripartite (SSC, TBS & CSE) are responsible for activities and deliverables to ensure the coordinated development of the GC-wide enterprise security architecture for implementing IT security across the GC in alignment with SSC initiatives. Other CITS and external DGs are informed on an as required basis.
0	6	**1.2 Security Standards**																									
E	7	GC security standards development	Security Standards Development applicable to all of GC led by TBS.	R	R	R	I	I	I	I									C	C			A			
E	8	Development of SSC Cyber & IT Security Standards for Mandated Services	Create and maintain SSC IT Security Standards for mandated services (DCC, TTP, ETI). Provide oversight for Security Artifacts / Standards development (Peer Review) relating to policy, architecture and standards development & tech writing in preparation for management approval stage. Oversight and management of 8-12 Standards (Branch Level, 3 from SM). includes Peer Review Process & Engagement with TBS & CSE.	A	A	A	R	R	R	R			C	C	R	I			C	C		C	C		Partners will be soliticited for voluntary participation in Peer Review of SSC CITS standards.	DG Security Management team is accountable for coordinating the security standards development process and oversight including peer review process. Depending on the specific standard, CITS DGs are responsible for the development of security standard within their specific areas of responsibilities. Other SSC Branches are consulted as the standards may impact the functions within their responsibility. The role of the Strategy/Architecture branch could be R or C as their role in standards process approval is not formalized at this time.
I	9	Peer Review process for SSC security standards and artifacts.	Provides a formally documented review process for CITS security standards and security artifacts, as well as standards and artifacts submitted for review by other parties.	A	A	A	R	R	R	R	C					C		I	C	C		C	C			DG Security Management team is accountable and responsible for the Peer Review Process definition and process oversight. CITS DG's representatives are responsible for the creation of the artifacts in their area of responsibility and for review and feedback. Enterprise Architecture/Strategy Branch, CSE and TBS are consulted depending on the subject matter of documents in review.
E	10	Partner Engagement: (a) CITS-Partner Interaction RACI (b) Support Partner Projects in Security Design and Assessment (SDA)	(a) Define ITS-related Processes, Guidelines, Roles and Responsibilities and RACI for partners on boarding on SSC infrastructure in a cloud-like security environment. (b) This function involves CITS support to the partner departments and clients in the design of security controls and providing SSC's assessment report as evidence for the Partner's SA&A activity.	A	A	A	I	I	I	I	I				C	I			C				I		Design and assessment of controls is limited in scope to those controls owned and operated by SSC.	DG Security Management is accountable. Security Program Engagement is responsible. CITS PM DG, Strategy Branch/Account Management, Partner's DSO and CIO are consulted. TBS is responsible for the TBS process for "Provider -Consumer" authorization. CSE can provide advice, guidance and, depending on the program, support in designing and assessing information system security. CSE also needs to understand the system and security design in order to assist in the cyber defence of GC networks.
0	11	**2.0 Security and Privacy by Design**																									
E	12	Security by Design and Integration: SSC IT Solutions (a) SSC Security Architecture (b) IT Security Controls for SSC Mandated Transformational Services (c) IT Security Controls for Departmental (e.g. Partners') Business Applications	Develop and continuously evolve CITS Security Reference Architecture and accompanying artifacts (e.g. SDDs, etc.); Includes update to the Security Framework. a) Security by Design & Integration: DCC/Data Centre, TTP /Telecom and ETI/WTD b) Security Integration into SSC processes (e.g. PGoF) c) Integration of partner applications with enterprise security controls	A	A	A	C	C	C	C			C	C	C	I	I		I	C	I		C		scope of SSC activity is limited to infrastructure/common controls leveraged by partner application systems. Our architecture/design services ensure that these systems plug into a secure environment, and that partner system architecture is compliant and interoperable with Enterprise architecture. Partners will be consulted as necessary regarding integration of their applications with enterprise controls.	Security Management DG is accountable for the security architecture evolution. SM Program Engagement Directorate is responsible along with the Security Architecture Directorate because of their involvement in the SbD and Security Architecture evolution as per the Business Plan. CITS DGs are consulted because of their dependence on this function. Strategy Branch/Architecture, CSE and TBS are also consulted.

SSC Cyber and IT Security RACI

RACI Definitions

R	Responsible	Responsible to do the work or part of it, (multiple R's may be assigned per task)
A	Accountable	Makes the final decision and has the ultimate ownership ... also does some work (only one A assigned per task)
C	Consulted	Must be consulted before a decision or action is taken ... (multiple C's may be assigned per task)
I	Informed	The person who must be informed that a decision or action has been taken

Version : 16w14.2

2016-04-05

R:\ITSB\CITS\02 Management\080 CITS Organizational Development\Organization and RACI

Request changes to:

SSC.citspeerreview-cstipeerreview.SPC@canada.ca

Sensitivity:
Protected A

Internal / External / Hide	Ref Line # (Gaps due to internal Funct. not listed)	Function	Function / Task Description	C 1	C 1	C 2	C 3	C 4	C 5	C 6	C 7	C 8	C 9	C 10	C 11	C 12	C 13	C 14	C 15	C 16	C 17	C 18	C 19	C 20	C 21	C 22
				SSC-Department (Highest Level)	**SSC-CITS Branch** (High Level)	**DG Security Management (Dinesh Mohan)**	**DG Cyber & IT Security Operations (Eric Belzile)**	**DG Infrastructure (Donald Messier)**	**Sr Dir. Identity & Access Management (Simon Levesque)**	**DG Secret Infrastructure (Dinesh Mohan)**	**Sr. Dir. PM (*Lucy Levesque... tbd*)**	**External to CITS but within SSC**	Service Management & Data Centres Branch (A/Patrice Rondeau)	Networks & End User Branch (Pankaj Sehgal)	Strategy Branch (Peter Bruce)	SSC Corporate DSO (A/Marc Contois)	Corporate Services Branch (A/Elizabeth Thrompi)	**(External to (SSC)** Partner Department,	Communications Security Establishment (CSE)	Public Safety (PS)	Royal Canadian Mounted Police (RCMP)	Treasury Board Secretariat (TBS) Chief Information Officer Branch (CIOB)	**Other** (See Notes)	**Notes-External**	**Notes-2**
																									Dynamic Information subject to frequent changes. This table is expected to continuously be updated as needed. Please continue to provide your feedback and change requests to the address provided in the version header box.	
E	13	Privacy by Design	Develop an Integrated Privacy by Design CITS framework and the supporting standards and processes for the Security Architecture Design in consideration of the business context and requirements and the SSC "Directive on Conducting Privacy Impact Assessments" ; Integrate with SSC SDLC and SSC processes; Define deliverables artifacts in support of ATIP and OPC legislated activities. 'Provide Privacy Assessment services: - Privacy Risk Checklist/Questionnaire; - Core Privacy Impact Assessment (PIA)	A	R	R									R		A		I	I			C		see note for item 13 (above)	Note: A newly - published draft of SSC "Directive on Conducting Privacy Impact Assessments" August 6, 2015 includes a detailed RACI for both Enterprise and Internal PIA. The entries in this RACI reflect this directive. DG Security Management is responsible for: • aligning IT security safeguards with privacy controls prior to authorizing the use of an IT system; • completing Privacy Risk Checklist for enterprise initiatives;
I	14	Datacentre Workload Migration security	Assess the application systems which are being migrated into the Enterprise Data Centre - advice and guidance, planning estimates, SRTM evidence, Risk assessments	A	A	A	R				C															SO responsible to perform a VA where requested as input for a risk assessment.
0	15	**3.0 IT Security Risk Management**																								
0	16	**3.1 Enterprise/Departmental IT Security Risk Management Process**																								
I	17	Risk Management Process	Maintain IT security RM process throughout System Life Cycle (SLC) and carry out continuous risk assessment, monitoring and maintaining authorization throughout operations, assessing threats, disposal phases, patch management, incident management, and other security risk management processes.	A	A	A	R	R	R	R			R	R		C		C	I			I			DG Security Management is Accountable. SM Security Program Architecture, and other CITS DG's and Service Branches are responsible within their respective areas of responsibility.
E	18	Enterprise/Departmental Security Risk Identification	Define and quantify IT Security risks inherent in the operation of GC systems (Privacy Assessment, Security Categorization, Concept Operation, Threat Assessment).	A	A	A	C									C		C	C			C		SSC needs to determine risks for our SA&A of common controls provided for systems, which in turn is an input to Partner's SA&A. Partner consultation is to obtain the information necessary (injury levels, threat profile, business needs for security) to do so. Partner is still accountable and responsible for assessing their own risks.	DG Security Management is Accountable. SM Security Program Architecture is responsible. Partners and SSC DSO are consulted along with CSE and TBS/CIOB.
I	19	Residual Risk Assessment	Identify residual risks and document, in the Risk Register, Security Assessment Report, Authorization Recommendation and Security Action Plan (SAP);	A	A	A	C	C	C	C	C		I	I	I	I		I	C			I			DG Security Management is Accountable. SM Security Program Architecture is responsible. CSE can provide advice, guidance and, depending on the program, support in determining residual risks. CSE also needs to understand the system and residual risks in order to assist in the cyber defence of GC networks.
I	20	Risk Remediation Process (Planning, Implementation, Monitoring)	Maintain IT security RM process throughout System Life Cycle (SLC) and carry out continuous risk assessment, monitoring and maintaining authorization throughout operations, assessing threats, disposal phases, patch management, incident management, and other security risk management processes	A	A	A	R	R	R	R			R	R		C		C	I			I			DG Security Management is Accountable. SM Security Program Architecture, and other CITS DG's and Service Branches are responsible within their respective areas of responsibility.
0	21	**3.2 System/Service IT Security Assessment & Authorization (SA&A) Process**																								
I	22	SA&A Process Management - Security Requirements	The SA&A process includes the following steps: 1. Preliminary Assessment of Security Requirements (Architecture Vison, IT Security Controls)	A	A	A	C	R	R	R	R								I			I			DG Security Management is Accountable. SM Security Program Architecture is responsible for assessment. SM is responsible for project management. CITS DGs are responsible for providing input for assessment for their respective services, including architecture and security controls documents. SO only consulted, they do not provide/decide on requirements, but will give SM a sanity check.
I	23	SA&A Process Management - SA&A Evidence	2. Prepare Evidence (Project Deliverables). System developers and architects are to prepare evidence documentation and supporting artifacts in accordance with the Security Plan for the submission to the security assessor.	A	A	A	R	R	R	R	R		R	R		I		I	C			C			DG Security Management is Accountable for the SA&A Process. SM Security Program Architecture and Security Program Engagement are responsible for the assessment. CITS DGs and SSC DCC and NEUD Branches are responsible for providing evidence for assessment for their respective services, including architecture, design documents, build books, SRTM, etc.
I	24	SA&A - Planning and Security Assessment	Assessment of evidence, identifying residual risks and preparation of the Security Assessment Report.	A	A	A	I	I	I	I	C		I	I		I		I				I			DG Security Management is Accountable for the SA&A Process. SM Security Program Architecture and Program Engagement are responsible for the assessment of their respective areas of responsibilities.
I	25	Authorization Recommendation to SRMB	Recommends authorization to the Authorizer (Record of Decision).	A	A	A	I	I	I	I	C		C	C		I		I				R			DG Security Management is Accountable for Authorization Recommendation based on the Security Assessment. SM Security Program Architecture and Program Engagement are responsible for
E	26	Authority to Operate (ATO) - SSC Mandated GC Services (SRMB)	Recommend Authority to Operate (ATO) for production of mandated GC Service (e.g. WTD, EUD, MSFTP)	A	A	R	C	I	I	I	C		C	C		I		I	I			I			ADM CITS is Accountable for recommending ATO to the responsible Operations Branch (DCC, Network and End User) DG SM is Responsible. CSE needs to understand the status of GC information systems in order to assist in the cyber defence.
E	27	Authority to Operate (ATO) - Departmental Applications	Recommend ATO for departmental business application (Including Legacy)	R	R	R	C				C		C	C		I		A				C			Partner department CIO is Accountable for recommending ATO to the responsible Operations Branch (DCC, Network and End User). DG Security Management is responsible for the assessment . TBS is consulted as part of their involvement in the Authorization process.
E	28	Authority to Operate (ATO) - Non-SSC Mandated, GC Services	Recommend ATO for production of non-mandated GC Services	R	R	R	C						C			I		I				A		These are GC common applications that are not part of SSC's mandate. Typically another department is the application or service provider, while SSC provides infrastructure. E.G. Shared Case Management System.	TBS CIOB is accountable for recommending Authorization
0	29	**Environmental Security for Mandated Services**																								

SSC Cyber and IT Security RACI

RACI Definitions

R	Responsible	Responsible to do the work or part of it, (multiple R's may be assigned per task)
A	Accountable	Makes the final decision and has the ultimate ownership ... also does some work (only one A assigned per task)
C	Consulted	Must be consulted before a decision or action is taken ... (multiple C's may be assigned per task)
I	Informed	The person who must be informed that a decision or action has been taken

Version : 16w14.2

2016-04-05

R:\ITSB\CITS\02 Management\080 CITS Organizational Development\Organization and RACI

Request changes to:

SSC.citspeerreview-cstipeerreview.SPC@canada.ca

Sensitivity: Protected A

Internal / External / Hide / 0 - Header / T -tbd / f-future /	Ref Line # (Gaps due to internal Funct. not listed)	Function	Function / Task Description	C 1 SSC-Department (Highest Level)	C 1 SSC-CITS Branch (High Level)	C 2 DG Security Management (Dinesh Mohan)	C 3 DG Cyber & IT Security Operations (Eric Belzile)	C 4 DG Infrastructure (Donald Messier)	C 5 Sr Dir. Identity & Access Management (Simon Levesque)	C 6 DG Secret Infrastructure (Dinesh Mohan)	C 7 Sr. Dir. PM (*Lucy Levesque... tbd*)	C 8 External to CITS but within SSC	C 9 Service Management & Data Centres Branch (A/Patrice Rondeau)	C 10 Networks & End User Branch (Pankaj Sehgal)	C 11 Strategy Branch (Peter Bruce)	C 12 SSC Corporate DSO (A/Marc Contois)	C 13 Corporate Services Branch (A/Elizabeth Thrompi)	C 14 (External to (SSC) Partner Department,	C 15	C 16 Communications Security Establishment (CSE)	C 17 Public Safety (PS)	C 18 Royal Canadian Mounted Police (RCMP)	C 19 Treasury Board Secretariat (TBS) Chief Information Officer Branch (CIOB)	C 20 Other (See Notes)	C 21 Notes-External	C 22 Notes-2
																										Notes-External	**Notes-2**
I	30	Physical Security Facility Assessments	Data Centre, Site & Telecom Room inspections, Certification Reports, Safeguard Implementation planning, RFP reviews, coordination with external agencies on behalf of SSC Mandated Services	A	A	A	I			C	R					I			C		R	C			**Dynamic Information subject to frequent changes.** This table is expected to continuously be updated as needed. Please continue to provide your feedback and change requests to the address provided in the version header box.	
I	31	Radiated Emissions Security (EMSEC) assessments for facilities	Planning, coordination, Assessments and Certification reports for EMSEC.	A	A	A	I	I		C	R					I			C		R	C				
0	32	**3.3 Supply Chain Integrity Management process**																									
E	33	Supply Chain Integrity (SCI)	Develop, manage and ensure adherence to the SCI process to: 1. Ensure that no un-trusted equipment, software or services are procured by SSC and are used in the delivery or support of GC services. 2. Ensure that the Supply Chain Security Information (SCSI), as provided by bidders to SSC, is submitted to CSE for assessment and that any business decisions to address products or services of concern is based on the supply chain risks, recommendations and mitigation measures as provided by CSE. 3. Ensure that SCI auditing is conducted throughout the life of the contract and that any products or services that may already be in use and are identified as having increased risk are properly addressed by SSC.	A	A	A	I						C	C		I	R		I	C			I	C*	Scope is limited to supplies and services that SSC is mandated to procure. Partners are accountable for their own procurements. *PWGSC is only consulted if Acquisitions is acting as procurement authority on behalf of special clients (e.g. TBS, RCMP). Per recent OiC, procurement authority for all IT related products and services have been transferred under	Note: SCI process is defined in the Supply Chain Integrity Standard v1.00 February 12. Additional details on various aspects are described in the tasks below DG Security Management is Accountable for the development and oversight of the SCI process and standard, Sec. Program Engagement is responsible along with the Strategy Branch/Procurement and vendor relationship (R) - security in contracting; CSE is consulted on product certification, SCSI assessment and TRAs; TBS is consulted; Service Branches are consulted on operational considerations. CITS Directorates General are consulted on architectural and design considerations.
I	34	SCI Product Procurement Management	Manage all aspects of competitive procurement process that is subject to the SCI process by: • Ensuring the application of SCI process to the applicable product or service, including Workplace Technology Devices (WTD); • Ensuring that that the process is covered by the SSC National Security Exception; • Creation of formal documentation and correspondence with prospective bidders; and • Ensuring that the RFP solicitation contains SCI assessment clauses and resulting contract clauses.	R	R	R	I									I	A		I	C					Corporate Services/ Procurement and Vendor Relationship (PVR) is Accountable and Responsible . DG Security Management / Security Program Engagement is Responsible for process coordination and interface with PVR and CSE; CSE is responsible for SCSI assessment and recommendations.
I	35	SCI Process Management (technical control)	Manage SCI process by: • Ensuring adherence to the SCI standard in accordance with the roles and responsibilities associated with this process; • Developing and ensuring inclusion of SCI clauses in the resulting contract; • Evaluation of SCSI by CSE and application of required mitigations from the resulting assessment; and • Ensuring that that any business decision to Accept/Reject competitive procurement is based on the supply chain risks, recommendations and mitigation measures as provided by CSE.	A	A	A	I									I	R		I	C			I		DG Security Management is Accountable for managing the technical aspects of SCI, Sec. Program Engagement is Responsible for management and coordination of the process. CITS Security Operations are Consulted. Strategy Branch/PVR is Responsible for procurement and contracting. CSE is Responsible for SCSI assessment and TRA on product certification,
H	36	SCI Audit Process	Manage the SCI Audit process by: • Inventorying all hardware, software or managed services in operation when identified as having increased risk; • Conducting a TRA (in conjunction with CSE) of the equipment identified on the inventory impact report; • Developing a mitigation plan to address identified risks.	A	A	A	C	I			R					I	C		I	R			I		DG Security Management is Accountable for overall coordination of CSI audit. Sec. Program Engagement is Responsible for, threat monitoring and CSI coordination. CITS Security Operations are Consulted. The DG of infrastructure is informed of the requirement due to their involvement with the inventory of infrastructure hardware and software. Strategy Branch/PVR is Responsible for CSI and vendor communications; CSE is Responsible for CSI assessment and TRA as well as providing advice and guidance on IT Supply chain risk and mitigation.
I	37	SCI Recall Process	Managing a Recall Process on all devices, software or managed services in operation when identified by SSC and CSE as having a supply chain risk. Includes: • Analysis and coordination of SCI threats and mitigation measures; • Preparing inventory impact and risk assessment reports; • Reviewing mitigation plan and assessing residual risk; and • Coordinating the implementation of the response.	A	A	A	C	I			R			R	R		C	C		I			I		DG Security Management is Accountable for the overall coordination of CSI recall process. Sec. Program Engagement is Responsible for analysis and coordination, risk assessment and process response/mitigation. CITS Security Operations are Consulted. Operations Branches are Responsible for the mitigation Plan implementation CSE is consulted on product certification, threat data advice and guidance.
E	38	Contract Security Review & Input Service	(a) When required, provide verification that the SRCL aligns to any applicable SCI requirements. (b) where required, provide IT security requirements to be appended to contracts or agreements. (c) review contracts or agreements as required/requested	A	C	R											I	A		I	C					see note for 35 (above).	SRCLs are used in the service contracting process and are not related to purchase of hardware or software. SRCLs are typically submitted to corporate security (or PWGSC) for review. If the SRCL indicates that there are IT Security requirements (i.e. The contractor will store or process GC information), then CITS will provide the ITS requirements.
0	39	**4.0 IT Security Performance & Compliance Management**	- - - - - - - - - - - - Future Development (here for completeness)- - - - - - - - - -																							

SSC Cyber and IT Security RACI

RACI Definitions

- **R** Responsible — Responsible to do the work or part of it, (multiple R's may be assigned per task)
- **A** Accountable — Makes the **final decision** and has the **ultimate ownership** ... also does some work **(only one A assigned per task)**
- **C** Consulted — Must be consulted **before** a decision or action is taken ... **(multiple C's may be assigned per task)**
- **I** Informed — The person who must be informed that a decision or action **has** been taken

Version : 16w14.2

2016-04-05

R:\ITSB\CITS\02 Management\080 CITS Organizational Development\Organization and RACI

Request changes to:

SSC.citspeerreview-cstipeerreview.SPC@canada.ca

Sensitivity: Protected A

Internal / External / Hide	Ref Line # (Gaps due to internal Funct. not listed)	Function	Function / Task Description	C 1 SSC-Department (Highest Level)	C 1 SSC-CITS Branch (High Level)	C 2 DG Security Management (Dinesh Mohan)	C 3 DG Cyber & IT Security Operations (Eric Belzile)	C 4 DG Infrastructure (Donald Messier)	C 5 Sr Dir. Identity & Access Management (Simon Levesque)	C 6 DG Secret Infrastructure (Dinesh Mohan)	C 7 Sr. Dir. PM (*Lucy Levesque... tbd*)	C 8 External to CITS but within SSC	C 9 Service Management & Data Centres Branch (A/Patrice Rondeau)	C 10 Networks & End User Branch (Pankaj Sehgal)	C 11 Strategy Branch (Peter Bruce)	C 12 SSC Corporate DSO (A/Marc Contois)	C 13 Corporate Services Branch (A/Elizabeth Thrompi)	C 14 (External to (SSC) Partner Department,	C 15 Communications Security Establishment (CSE)	C 16 Public Safety (PS)	C 17 Royal Canadian Mounted Police (RCMP)	C 18 Treasury Board Secretariat (TBS) Chief Information Officer Branch (CIOB)	C 19 Other (See Notes)	C 20	C 21 Notes-External	C 22 Notes-2
																										Dynamic Information subject to frequent changes. This table is expected to continuously be updated as needed. Please continue to provide your feedback and change requests to the address provided in the version header box.	
f	40	5.1 Branch Performance Management & Reporting	Effectiveness and ability of organization to successfully manage Cyber and IT Security. This is an indicator and enabler for Cyber and IT Security Maturity for GC	A	A	A	R	C	C	C			R	R	C	I			I	C	I	I	R			
f	41	Performance Management Framework and Methodology	Develop a Performance Management Framework and Methodology to measure the efficiency and effectiveness of security measures applied to the SSC information systems and security programs at the enterprise, program and security control levels.	A	A	A	C	C	C	C			C	C	C	I			I	C			C			This initiative and the detailed activities described in the rows below is deferred to 2016.
f	42	IT Security Performance Metrics	Define and quantify IT Security performance Metrics including Security Control Objectives (SCO) and Key Performance Indicators (KPI) for a quantifiable measurement to track the progress in achieving specific security objective. SCO and KPI can be defined at various levels : i.e. enterprise, program, system and specific security control. Define IT Security metrics to measure KPIs based on the results of data collection, analysis and reporting.	A	A	A	C	C	C	C			C	C	C	I			I	C			R			This initiative is deferred to 2016. CSE can provide advice, guidance and, depending on the program, support in determining IT Security performance metrics.
f	43	Performance Reporting	Design, develop, deploy and maintain reporting vehicles (dashboards), tools and information repository to present, in real time (or on a periodic basis), the status of key IT security performance indicators on security posture, issues and remediation. The reporting should be at the various levels of granularity ensuring that all interested parties are consulted and informed.	A	A	A	C	I	I	I			I	I	I	I			I				I			
f	44	Issues Remediation	Develop methodology, processes and procedures to assess, react and remediate detected security issues to maintain an overall SSC enterprise and/or a specific ITS Program's Security Posture.	A	A	A	R	C	C	C			C	C	I	I			I	I	I	I	I			
f	45	Configuration Change Management Review (Security review and Authorization of Network, Server and OS changes which may impact security)	Security Authorization of changes where security may be impacted by network/server/app changes as reviewed by Service Management CAB. (includes new applications going into production)	A	A	I	R	C	C	C			R	R		I			I							SSC/CITS/Sec-Ops should be the primary (This is a new line added 2015-10-08 as network changes and Security engagement needs to be integrated within ITIL processes.
f	46	5.2 Compliance Management	The means by which Audits are performed in order to gather compliance to policy instruments provided by both TBS and SSC specific instruments. (Policy, Standards, Directives)	A	A	A	R	R	R	R			C	C	I	R			R	I			C			
f	47	Security Controls - Compliance Verification and Validation	• Verification: Define and implement a process to verify that the equipment, software and processes associated with the security control are designed, built and implemented according to the specifications and requirements. • Validation: Define a process to validate that a security control is operating as intended, that it produces the expected results and that the security control will continue to operate as intended in the future. The validation results comprise the collection of documented evidence. 'Conduct Security Controls Compliance	A	A	A	R	R	R	R			C	C	I					I			I			Security Management DG is accountable for the definition of Security Controls Compliance Processes in consultation with other CITS organizations; 4 CITS Organizations are responsible for the execution of security controls validation and for continuous monitoring of the security controls post authorization.
f	48	Security Controls - Compliance Monitoring process/standard	Process: Develop compliance monitoring processes and/or standard for continuous compliance monitoring of security controls as defined in the "Security Controls Compliance - Verification and Validation",	A	A	A	R									R			R	I			C			Not clear why TBS was designated as Accountable in the 2014 RACI. This is not in line with the definition. Security Controls Compliance is the accountability of Security Management with the CITS Directorates responsible as well as partners' and SSC DSOs. (TBD) CSE must understand the status of GC information systems in order to assist in the cyber defence
f	49	Compliance with Regs and Standards	Security Compliance Monitoring / Audits	A	A	A	R	R	R	R	R															
f	50	5.3 Security Audit Responses / Support (For SSC-CITS targeted requests from AEB & MAF)	Activities relating to supporting Audit requests from AEB, MAF. Preparation of SSC positions in relation to Audit questions and updates.	A	A	A	C	C	C	C							R						C			
f	51	Audit Management - define and implement audit process	Define and implement a process whereby an independent auditor can verify that the system/service conforms to the SSC security; policies, directives and standards; 'Conduct GC Audits (MAF, OAG, TBS, Investment Canada reviews, Other)	A	A	A	C	C	C	C							R						C			All CITS DGs are consulted on the Audit process for which they may be required to provide input to the auditor and/or ongoing reporting. TBS will be consulted on the format and content of the GC audit reports. The actual conduct of audits should be the responsibility of the SSC Audit group in SSC Corporate Services. (TBD)
0	52	**5.0 Security Operations**																								
E	53	SSC Security Operations Centre is mandated to provide 24/7 IT Security services including monitoring, detection, incident handling, coordination and recovery services in support of Canada Cyber Security Strategy to protect Government of Canada's information assets (up to and including Secret) from exploitation, unlawful access, or data theft and to aid in the recovery of services affected in the act of these cyber-attacks. IT security operations capabilities are bolstered through the coordination of IT security incidents within the greater context of the GC (GC-CIRT), a Federated Information Protection Center that provides continuous analysis, assessment, and review of security related data (FIPC), a highly specialized IT security incident recovery team (IT-SIRT) and Vulnerability Management Services (VMS).																								
E	54	Cyber Monitoring Strategy Development for SSC Mandated Services	Responsible for the strategic development of the Cyber Defense strategy for SSC. Accountable to develop the Cyber Defense capability requirements by analyzing the current effectiveness of the tools and systems, analyzing the trends of cyber threats, determining gaps and priorities in the need for new capabilities to better defend GC networks. Work with GC organizations engaged in Cyber Defense activities to ensure alignment, avoid duplications and ensure our respective capabilities are complementary to defend the GC systems. Engage and provide guidance and strategic direction to SSC partners in support of their IT Security mandate.	A	A	C	A	I	I	I									C	C	C	C		C*	C: CRTC C: DND C: CSIS	To be detailed by Area of Accountability

SSC Cyber and IT Security RACI

RACI Definitions

R	Responsible	Responsible to do the work or part of it, (multiple R's may be assigned per task)
A	Accountable	Makes the final decision and has the ultimate ownership ... also does some work (only one A assigned per task)
C	Consulted	Must be consulted before a decision or action is taken ... (multiple C's may be assigned per task)
I	Informed	The person who must be informed that a decision or action has been taken

Version : 16w14.2

2016-04-05

R:\ITSB\CITS\02 Management\080 CITS Organizational Development\Organization and RACI

Request changes to:

SSC.citspeerreview-cstipeerreview.SPC@canada.ca

Sensitivity: Protected A

Internal / External / Hide	Ref Line # (Gaps due to internal Funct. not listed)	Function	Function / Task Description	C 1 SSC-Department (Highest Level)	C 1 SSC-CITS Branch (High Level)	C 2 DG Security Management (Dinesh Mohan)	C 3 DG Cyber & IT Security Operations (Eric Belzile)	C 4 DG Infrastructure (Donald Messier)	C 5 Sr Dir. Identity & Access Management (Simon Levesque)	C 6 DG Secret Infrastructure (Dinesh Mohan)	C 7 Sr. Dir. PM (*Lucy Levesque... tbd*)	C 8 External to CITS but within SSC	C 9 Service Management & Data Centres Branch (A/Patrice Rondeau)	C 10 Networks & End User Branch (Pankaj Sehgal)	C 11 Strategy Branch (Peter Bruce)	C 12 SSC Corporate DSO (A/Marc Contois)	C 13 Corporate Services Branch (A/Elizabeth Thrompi)	C 14 (External to (SSC) Partner Department,	C 15 Communications Security Establishment (CSE)	C 16 Public Safety (PS)	C 17 Royal Canadian Mounted Police (RCMP)	C 18 Treasury Board Secretariat (TBS) Chief Information Officer Branch (CIOB)	C 19 Other (See Notes)	C 20	C 21 Notes-External	C 22 Notes-2
																										Dynamic Information subject to frequent changes. This table is expected to continuously be updated as needed. Please continue to provide your feedback and change requests to the address provided in the version header box.	
E	55	Prevention for SSC Mandated Services (Minimizing vulnerabilities of the SSC Infrastructure supporting the 43 partners)	Central point of contact for the coordination, reporting and trending analysis of cyber security events that may have impacted or may impact the GC. Gathering and analysis of data or information within the domain of Cyber and IT Security and reciprocal sharing and analysis of intelligence information. Dissemination of actionable cyber threat indicators and intelligence, community threat-sharing and synthesization of situational awareness information. Monitor vendors vulnerability information publications and determining action plans accordingly. Provide vulnerability assessment scans of new systems for the purpose of SA&A.	A	A	I	A	C											C	R				C*		On-Demand VM Scans on partner applications and desktops, otherwise scheduled VA limited to infrastructure and server OS. C: Non-Partner Dept./Agency R: CSE is responsible to provide threat intelligence.	
E	56	Detection / Response / Recovery for SSC Mandated Services (Managing incidents occurring on the SSC infrastructure supporting the 43 partners)	Undertake Cyber Defence activities related to monitoring and detection of IT security events . Sharing a broad view of the threats, threat actors, different attack types and vulnerabilities affecting all GC departments. Coordination of all phases of event management for security events that have impacted the GC. Incident coordination and response within the SSC Partners' networks. Providing guidance and mitigation advice for cyber incidents to SSC Partners. Conduct Cyber and IT Security incident forensic analysis and investigations for SSC partners. As a first responder, lead recovery efforts of complex and/or widespread Cyber and IT Security incidents. Develop long term mitigation solutions, and provide VA scans and compliance reports in support of security incident management.	A	A		A	C						I			I		C	I	I	I			C: Partners are consulted prior to response and recovery activities.	
I	57	Operational Internal Security Reporting	All activities and functions associated with internal reporting requirements. Short and Long term trending, and incident reporting metrics, co-ordination and reporting on Security Operations KPI, and analytics assessments - related to strategic planning.	A	A	I	A																		
I	58	Operational Security Project Support	All activities and functions associated with planning and support of all Cyber and IT Security projects (transformational).	A	A	C	R	C	C	C	A														
I	59	IT Operations Situational Awareness	All activities related to qualifying and quantifying the structure of SSC networks, types of computing assets deployed and likely threats against those systems, supported missions, business functions, and general sense of attack surface.	A	A		A																		
0	60	**5.1 Infrastructure Security (IS)**																							
E	61	Infrastructure Services (IS) is responsible for the overall definition and delivery of tools and services for infrastructure protection. It identifies and prioritizes control requirements, balancing security, cost and resource constraints; engineers approved controls; then builds and delivers them to operations for deployment into the SSC production environment. (Firewalls, IDS, IPS, etc.)		A	A	C	C	A	C	I			R*	C	I	C	I		C	C			I		* SMDC Branch responsible for physical installation only.
I	62	IS: Network Security (firewalls, web filtering, IPS/IDS, zoning)	Provide support for Firewalls in the form of initial implementation, ongoing support and decommissioning. Web filtering software is installed and maintained by this group. Data Loss Protection (DLP) is managed partially by this group. Its management includes implementation and software maintenance of the COTS products that support it through the application of engineering changes.	A	A	I	C	A	C	I	-		R	C	I	C	I		C	-	-	-	-		Infrastructure security is responsible for all activities around IT security componenets on the SSC network up to and including the installation of the unit on site. Their activities including the gathering of requirements, the formulations of spewcifications and the identification of specific componenets that meet the specification. The group then acquires the equipment, configures it, applies all requires engineering changes and fixes and plans the installation in the field. Upon completion, the unit is turned over to operations for day to day monitoring. Operations notifies support in the event of equipment failure. This groups only role during the units steady state operation is to receive and apply any new engineering changes or fixes.
I	63	IS: Network Access (NAC, VPNs, secure extranet)	This group installs and maintains the Virtual Personal Network (VPN) service. The ongoing support includes the application of any fixes received by the vendors. Secure Extranet is provided and maintained by this group and provides controlled access to partners and vendors to specific components of internal systems without exposing the entire system.	A	A	I	C	A	C	I	-		R	C	I	C	I		C	-	-	-	-		as per note for item 85 (above)
I	64	IS: Anti-malware (anti virus, anti-spam, anti-phishing)	This group installs and maintains the anti-malware on servers. Installation includes planning, customization, and the application of engineering changes tied to the malware profiles. Maintenance includes the ongoing application of new engineering changes tied to the new malware appearing.	A	A	I	C	A	C	I	-		C	C	I	C	I		C	-	-	-	-		as per note for item 85 (above)
I	65	IS: Deploy and Maintain Advanced Persistent Threat Safeguards	The deployment of tools, techniques and methodologies to protect against Advanced Persistent Threats. This includes determining component atrributes, configurations and installation based on existing architectures, IT security policies and best industry practices.	A	A	I	R	A	C	I	-		R	C	I	C	I		C	C	-	-	-		as per note for item 85 (above)
I	66	IS: Deploy and Maintain SIEM system	Monitoring SIEM logs to monitor event sequences that indicate a potential security incident, and taking remedial action to investigate and respond. SIEMs collect a vast quantity of operational logs; the security incident monitoring component is only looking for sequences that indicate deliberate malicious activity.	A	A	I	R	A	C	I	-		C	C	I	C	I		C	-	-	-	-		as per note for item 85 (above)
I	67	IS: Procurement of IT security networking equipment and services	This group formulates the specifications for equipment , software and services required to fulfill SSC's mission to protect the network perimeter as well as the internal components from internal and external threats.	A	A	C	C	A	C	I			C	C	C	C	C							
I	68	Maintenance and support of Enterprise Security tools	Break/fix, licence management, hardware/software technical support.	A	A		C	A																IS-owned equipment only
I	69	Security Log Source Management	Log source acquisition* and management.	A	A		C	A																* Acquisition means setting up the interface between the log source (e.g. a server) and the SIEM
I	70	IT Operations Availability Monitoring of Enterprise Sec devices	Up/down monitoring of system components and performance monitoring (CPU, capacity, etc.).	A			I	C					A											TBD: not sure who is currently doing this, need to engage with SMDC Branch
I	71	Provision of operational monitoring facilities for Enterprise Sec devices	Source and configure the components for monitoring for the use of Networks operations	A	A			A					C											IS-owned equipment only
0	72	**6.0 Identity and Access Management (IAM) Services**																							

SSC Cyber and IT Security RACI

RACI Definitions

R	Responsible	Responsible to do the work or part of it, (multiple R's may be assigned per task)
A	Accountable	Makes the final decision and has the ultimate ownership ... also does some work (only one A assigned per task)
C	Consulted	Must be consulted before a decision or action is taken ... (multiple C's may be assigned per task)
I	Informed	The person who must be informed that a decision or action has been taken

Version : 16w14.2

2016-04-05

R:\ITSB\CITS\02 Management\080 CITS Organizational Development\Organization and RACI

Request changes to:

SSC.citspeerreview-cstipeerreview.SPC@canada.ca

Sensitivity: Protected A

Internal / External / Hide	Ref Line # (Gaps due to internal Funct. not listed)	Function	Function / Task Description	C 1 SSC-Department (Highest Level)	C 1 SSC-CITS Branch (High Level)	C 2 DG Security Management (Dinesh Mohan)	C 3 DG Cyber & IT Security Operations (Eric Belzile)	C 4 DG Infrastructure (Donald Messier)	C 5 Sr Dir. Identity & Access Management (Simon Levesque)	C 6 DG Secret Infrastructure (Dinesh Mohan)	C 7 Sr. Dir. PM (*Lucy Levesque... tbd*)	C 8 External to CITS but within SSC	C 9 Service Management & Data Centres Branch (A/Patrice Rondeau)	C 10 Networks & End User Branch (Pankaj Sehgal)	C 11 Strategy Branch (Peter Bruce)	C 12 SSC Corporate DSO (A/Marc Contois)	C 13 Corporate Services Branch (A/Elizabeth Thrompi)	C 14 (External to (SSC) Partner Department,	C 15	C 16 Communications Security Establishment (CSE)	C 17 Public Safety (PS)	C 18 Royal Canadian Mounted Police (RCMP)	C 19 Treasury Board Secretariat (TBS) Chief Information Officer Branch (CIOB)	C 20 Other (See Notes)	C 21 Notes-External	C 22 Notes-2
																										Notes-External	**Notes-2**
																										Dynamic Information subject to frequent changes. This table is expected to continuously be updated as needed. Please continue to provide your feedback and change requests to the address provided in the version header box.	
E	73	My Key and Internal Credential Management (ICM)	a TBS mandatory GC-wide public key infrastructure service that facilitates authentication for secure access to applications and Government of Canada networks	A	A	I	I	I	A	I	C									C			C		RACI assignments based on daily provision of steady-state services. Projects to upgrade these services will involve much consultation with other groups in SSC, TBS, CSE and Partners.	Given the nature of ICM, TBS and CSEC will be consulted on changes that impact the service from a business and security point of view.
E	74	Cyber Authentication	External Credential Management (ECM) - a TBS mandatory service, providing level of assurance 2 (LoA2) authentication services to Canadians, businesses and individuals when interacting with Government of Canada online services	R	R	I	I	I	R	I	C									C			A		TBS as business owner. See ext note for item 75.	Given the nature of ICM, TBS and CSEC will be consulted on changes that impact the service from a business and security point of view.
E	75	Enterprise Directory Services	provides the services to create and life cycle manage digital identities providing access and authorization to resources under SSC mandate	A	A	I	I	I	A	I	C									C			C		See ext note for item 75.	The user account and access lifecycle management activities will involve the clients (or partners) and service leads.
E	76	Enterprise Management of Identity, Control and Access (Infrastructure)	Provides the infrastructure,(Infrastructure as a service) Disciplines for people, processes, systems and technologies to assure the right individuals access the right resources at the right times for the right reasons, and to meet compliance requirements. Includes: SSC Identity and access control	A	A	I	I	I	A	I	C												I		See ext note for item 75.	These activities are done within existing frameworks of SSC/GC.
E	77	Departmental Management of Identity, Control and Access (Applications)	Management of Identity attributes of applications	R	R	I	I	I	R	I	C								A				I		See ext note for item 75.	These activities are done within existing frameworks of SSC/GC.
E	78	Management of Identity, Control and Access (GC Standards and Strategy)	Government of Canada Identity Standards and GC Strategy	R	R	I	I	I	R	I	C								I	C			A		See ext note for item 75.	These activities are done within existing frameworks of SSC/GC.
E	79	Public SSL Certificates	Service that leverages a commercial SSL certificate provider to issue SSL certificates used to secure public facing GC web sites in support of various services	A	A	I	I	I	A	I	C												I		See ext note for item 75. ICM service offering includes internal TLS certificates.	Changes to the service may need to disseminated to the client base,
0	80	**Security Project Management (PM):**	- - - - - - - - - - - Internal to SSC, here for completeness - - - - - - - - - - -	A															R							Decision to remove from External View (CITS/SM DG 2016-01-27)
I	81	Management Services for CITS Lead projects	Providing Project Management services for CITS Lead projects. (PM Leadership, management/coordination/ tracking/ delivery)	A	A	C	C	C	C	C	A		C						R							PM Oversight team provides day-to-day management, coordination and tracking CITS service relates requests for CITS activities by providing a 'single window' into CITS for project support and capacity
I	82	Security Project Intake	Provide Management Oversight (PMO) coordination and tracking of CITS Service requests. (coordination into the various security teams based on CITS Security Teams. - Intake / Request Management - Internal CITS Service Catalogue - Capacity Demand management - Reporting and tracking	A	A	C	C	C	C	C	A		C						R							• Intake / Request Management Working with the Enterprise Business Intake and Demand Management team within SSC and the Service Delivery Managers, the CITS PMO provides a front door for partner initiated request which require CITS related services. The PMO will coordinate internally within CITS to ensure the required service lines are engaged for input and assessments. • Internal CITS Service Catalog
0	83	**7.0 Secret Infrastructure (SI):**																								
E	84	Secret Infrastructure Transformation	Plan the evolution to design and implement a single, modern and enterprise-wide classified solution to consolidate and converge existing legacy classified information and voice systems.	A	A	C	C	C	C	A									C	C			C		Partners will be solicited for their requirements for transformation.	To be detailed by Area of Accountability
E	85	Communications Security (COMSEC) transition planning	Transition to an enterprise service to centralize and consolidate existing COMSEC functions and equipment for the GC's IT infrastructure, information and client services.	A	A	C				A						C			C	C*			C		* pending discussions between CITS SI Directorate and CSE.	To be detailed by Area of Accountability
E	86	Legacy Secret Operations	Conduct an in-service support deep dive to identify resources, roles and responsibilities, time allocation and an architectural overview of each network. Continue operational support of systems within SSC Scope	A	A	C				A									A*	C			C		A* in the process of transitioning accountability. Will become an R once completed.	To be detailed by Area of Accountability
I	87	Project Support - Secret Information Systems	Legacy and partner Secret network projects. Transformation and GCSI evolution projects.	A	A	C	C	I		A	R									C						To be detailed by Area of Accountability
I	88	GCSI Service Operations and Management	Ongoing in-service support of iGCSI On-board new partner departments Configuration Management Develop SI Service Catalogue	A	A	C	R			A			C	C												To be detailed by Area of Accountability
0	109	**8.0 Example Partner Department Security Functions**																								
E	110	Departmental Application Security	Design and develop (or acquire and customize) secure applications. Monitor application logs for anomalous behaviours.	C															A	C			C			
E	111	End-point/User Device Security	Hardening and managing user devices. Monitoring for, and responding to, endpoint malware infections.	C										R*					A	C			C		*SSC NEU Branch responsible for hardening telephony devices. Partners remain accountable for selecting the security level of their BlackBerry devices.	

Shared Services Canada | Services partagés Canada

Building the Government of Canada's Digital Platform

A consultation to update Shared Services Canada's Information Technology Transformation Plan

Service / Innovation / Value

Canada

CONTENTS

INTRODUCTION

Building the Government of Canada's Digital Platform provides an overview of Shared Services Canada's (SSC) plan for continuing the modernization of the Government of Canada's information technology (IT) infrastructure. This includes the email, data centres, telecommunications, network and IT security services that underpin federal operations and support the delivery of government services to Canadians.

This document provides an overview of the IT transformation agenda and poses questions on what an updated agenda should include and what it should deliver. We are seeking your feedback.

SSC's IT Transformation Plan is the infrastructure component of the IT priorities for the Government of Canada aligned with the *IT Strategic Plan*. Government IT priorities, including departmental IT plans, the *Cloud Adoption Strategy*, and the consultations leading to an updated *Cyber Security Strategy*, all fit together.

What is the IT transformation agenda?

SSC's IT transformation agenda is the roadmap to modernize the Government of Canada's IT infrastructure and delivery of IT services. SSC delivers email, data centres, network, 24/7/365 cyber-security protection, and workplace technology device services to departments and agencies in a consolidated and standardized manner to support the delivery of Government of Canada programs and services. With a whole-of-government approach to IT infrastructure services, SSC is generating economies of scale to deliver more efficient, reliable and secure IT infrastructure services.

We are seeking your views

SSC's IT Transformation agenda was first established in 2013, and SSC has since made progress in realizing its ambitious vision. The government context and the technology landscape have evolved substantially since 2013 as information technology systems and processes require continual refresh and evolution. While the benefits of an enterprise approach remain clear, SSC must update its agenda to ensure success in meeting near- and long-term government priorities.

SSC is seeking feedback on its IT service delivery and transformation goals and updated implementation plans by reaching out to:

- SSC employees
- Employees in customer organizations
- Industry, especially companies in the information and communications technology field
- Canadians with an interest in IT and large modernization projects

How to participate

There are different ways you can provide your views:

- Visit ittransformationconsultation.ca and provide your feedback through the interactive consultation workbook.
- Provide your feedback before October 31, 2016 by email to: consultations@ipsos.com

SSC will review all input. A variety of perspectives will assist the Department in its efforts to renew the transformation agenda. SSC will post online a summary of the feedback received in a “What We Heard” document in November 2016.

The consultation report will also be provided to the Independent Review Panel. This panel is reviewing SSC’s IT Transformation Plan to ensure IT consolidation initiatives are managed in a way that allows departments and agencies to deliver programs and services to Canadians effectively, efficiently and securely.

SHARED SERVICES CANADA'S INFORMATION TECHNOLOGY TRANSFORMATION PLAN

Building the Government of Canada's Digital Platform

In its 2015 *Speech from the Throne* and in *Budget 2016*, the Government of Canada presented its vision for pursuing real and meaningful change for the country. This includes a commitment to openness and transparency in all federal operations, to ensuring Canadians' security, and to stimulating economic growth through sustainable investments in the nation's infrastructure. This is fully aligned with the public service's Blueprint 2020 call to action to establish the digital, high-performing workforce of the future, making smart use of technology.

Shared Services Canada (SSC) is critical to realizing this collective vision, given its mandate to deliver the Government's foundational data centre, network, email, workplace technology and cyber and IT security services. These services represent the IT backbone underpinning federal service delivery to Canadians. Every time Canadians cross the border; every time they apply for Employment Insurance; every time they look to government action in the wake of emergencies like the Fort McMurray wildfires; even every time they check tomorrow's weather forecast—SSC is there, connecting Canadians to their government and ensuring federal services are delivered securely when they are needed, where they are needed, and without delay. In short, SSC's success is vital to all government operations by providing the technological infrastructure to respond to Canadians' needs.

SSC is mandated to deliver reliable IT infrastructure services so government can deliver programs and services to Canadians. Maintaining daily operations has thus been paramount from day one. This imperative was all the more pressing given the aging and highly fragmented IT infrastructure SSC inherited, a reality best underscored in the Auditor General's *2010 Spring Report*. As the report noted, this environment was at high risk of service failure and exposure to cyber-attacks, particularly as key pieces of equipment were no longer manufactured or supported by the manufacturers.

Government of Canada IT environment prior to 2011	SSC's IT transformation outcomes – Transform how the Government of Canada manages its IT infrastructure
• Lack of a common vision for Government of Canada IT infrastructure	• A shared Government of Canada vision for a digital government and IT infrastructure that supports it

• Systems and equipment becoming obsolete and little investments toward renewal
• Limited connectivity due to different platforms and systems
  • 63 different email systems with no common standard for platforms or addresses
  • 543 inefficient and vulnerable data centre sites
  • 50 outdated and silo-built wide area telecommunications networks
	• Improved reliability and connectivity brought about through common systems
	  • Deploying a single government-wide email system with a common *@canada.ca* naming convention
	  • Establishing fewer data centres that are secure, state-of-the-art and designed to meet high security and reliability standards
	  • Modernizing the Government's telecommunications services, including establishing a common, reliable, more secure and high-speed wide area network

• Residual risks for government data integrity and increased risks to citizens' data. • Risk of system failure and increased cyber-security exposure	• Security of systems, data and resistance to cyber attacks • Establishing a strengthened enterprise IT cyber-security platform that protects government information assets and ensures secure information flows, including between Canadians and government services
• Decentralized procurement of common workplace technology software and hardware	• Strong buying/purchasing power that will lead to economies of scale and better value for Canadians • Consolidating workplace technology hardware and software purchases across government, thereby translating the Government's buying power into the highest possible value for the Canadian taxpayer

The scale, scope and complexity of this plan are ambitious, and have few parallels in Canada or abroad, demanding unprecedented government-wide orchestration, innovation and synchronization.

SSC is making progress in achieving its objectives:

- More secure and effective data centres have been established.
- Contracts to consolidate the Government of Canada's wide area network have been awarded.
- The transition to one email system across government is underway.

Achievements to Date*

Some Highlights

- Closed a total of 62 data centres
- Installed 97,718 desktop phones with Voice-over Internet Protocol (VoIP) technology
- Provided Wi-Fi service to 30,729 public servants
- Enterprise videoconferencing now available to all 43 departments
- Established Security Operations Centre, instituted security-by-design and implemented Supply Chain Integrity

**As of March 31, 2016*

SSC is putting increased emphasis on client service, sound financial management and ensuring accountability through a revised business model focused on people, service, financial and project management and integrated cyber-security protection.

Managing the IT environment – A shared responsibility

There are several departments responsible for governing the IT environment throughout the Government of Canada, each with varying responsibilities:

The Treasury Board of Canada Secretariat (TBS), supported by the Chief Information Officer Branch, develops strategy and sets government-wide policy and mandatory requirements for IT and cyber security, and provides guidance on implementing the direction. TBS sets government-wide strategic direction for IT, with input from deputy ministers, chief information officers and other stakeholders. The responsibility for delivering IT services is shared between government organizations and central IT service providers, such as SSC and Public Services and Procurement Canada (PSPC).

Departments and agencies are responsible for managing their department-specific applications, as well as for developing information management policy instruments in alignment with Treasury Board direction.

Public Services and Procurement Canada provides IT supporting services, such as human-resource management systems, pay and pension, enterprise records and document management, and financial systems and services. SSC and PSPC jointly support federal organizations in procuring IT goods and services.

Shared Services Canada has the mandate to provide data centres, networks and email services to the largest government departments. Smaller government organizations receive these services on an optional basis. SSC, the Communications Security Establishment and Public Safety Canada have a shared responsibility for cyber and IT security, with oversight provided by TBS. In addition, SSC is responsible for procuring hardware and software, including security software for workplace technology devices—the authorized physical devices and related software used in government office work.

Getting the Foundation Right – SSC's evolved Integrated Business Model

The benefits of a government-wide approach to delivering and modernizing IT infrastructure services remain clear. Likewise, SSC's vision for establishing a modern, secure, efficient and reliable IT infrastructure remains sound.

However, the scale and scope of SSC's transformation agenda is ambitious and depends on a host of external and internal factors for success. This includes:

- industry's ability to supply the required solutions;
- SSC's capacity to deliver services and its customers' readiness to transition while also delivering on their own mandates and departmental priorities;
- stabilizing older IT equipment and systems, which is taking longer than expected; and
- managing the rising demand for SSC services year-over-year.

Collectively, these challenges underscore the need for fundamental organizational and strategic change to ensure SSC's success going forward. This includes an increased focus on service-management rigour and financial sustainability, alongside the pursuit of more realistic transformation timelines in full alignment with customer and industry capabilities and capacity.

SSC is also evolving its business model to better support an organization-wide focus on service delivery excellence and financial and project management throughout operations. Five organizational management disciplines guide the Department's path forward:

1) **People Management**: Building the skilled human capacity SSC needs to achieve its IT service delivery and modernization goals, both now and in the future. Workforce planning, recruitment, ongoing learning and development and employee enablement are some of the measures that will be undertaken.

2) **Financial Management**: Establishing a clear and transparent costing and pricing strategy that fully accounts for new and ongoing service demand and supports a formal capital replacement program to address the challenges with end-of-life, end-of-service IT equipment.

3) **Project Management**: Upgrading the project-management regime to ensure effective governance, integrated planning, and timely organizational capacity, enabling SSC to optimize the value delivered by its projects, embrace new technologies, and ultimately meet rising demand for ever-faster, capable and more secure digital services.

4) **Service Management**: Adopting a more holistic, customer-centric approach to providing daily services and delivering on transformation activities, supported by a revamped Service Management Strategy, enterprise tools and processes, and a dedicated program, all designed to improve service delivery going forward.

5) **Security Management**: Adopting a security-by-design approach throughout operations, alongside delivering the trusted, protective and resilient enterprise-level security services needed to achieve the Government's federal IT security vision and outcomes, ensures trusted delivery of federal programs, and protects Canadians' privacy and their data.

Questions: Implementation of management strategies:

- *People management: What additional workplace and workforce initiatives are required?*
- *Financial management: What approach should be adopted to measure progress, demonstrate benefits and report progress to customers, parliamentarians and to Canadians?*
- *Project management: What measures need to be in place in SSC and in customer organizations to deliver integrated project planning?*
- *Service management: What new tools and processes are required to deliver on SSC's "as-a-service model"?*
- *Security management: How should SSC be delivering its "security by design" approach for 24/7/365 protection against cyber-security threats?*
- *Are there other areas that SSC should add for additional focus?*

Action plans to implement the People, Financial, Project, Service and Cyber Security strategies will be developed and informed by the IT transformation agenda consultations, by the advice from the Independent Review Panel and ongoing engagement with SSC staff and customer organizations.

Revamping the Roadmap

A vision is nothing but a good idea unless supported by a solid strategic plan to translate vision into reality. The updated IT transformation agenda, informed by the work of the Independent Review Panel, and the broad-based consultations with staff, customer organizations and industry will fulfil this purpose by presenting SSC's realistic and actionable plan for realizing its vision. By delivering the IT Transformation Plan, SSC will address the challenges encountered to date, and ultimately move the Government from an increasingly unreliable and costly environment to a simpler, smarter and more secure government-wide IT platform and service delivery model.

Organizational Transformation – Service is the First Priority

First, SSC wants to ensure its programs and services reflect an enterprise-class service delivery organization. SSC can realize this vision by implementing the plans under its People, Financial, Project, Service and Cyber Security strategies, and by generally embracing a "service first" philosophy and an "as-a-service" model to deliver the right services at the right time. To achieve its "service first" model, SSC is using service delivery tools, such as:

- Clear service targets, such as service hours, service availability and the time required to restore services
- A consistent customer experience and customer-driven demand management regime
- Full customer visibility over the state of their services

In this target state, SSC would act not only as a service provider, but also as a service broker for high-value IT infrastructure services, delivered either by SSC or by private industry. In all cases, services would be delivered in a timely fashion and would meet customers' highest standards of security and confidentiality, integrity and availability. At the same time, SSC would offer advice

Question:

To achieve its "service first" model, what other tools should SSC consider using?

and guidance to support its customers in developing strategies and services, addressing the needs of today, while preparing to meet those of tomorrow. Throughout, SSC wants to operate as a single entity, supported by modern service-management tools and processes and organized to serve government as a single enterprise while working to meet the needs of each organization.

Technological Transformation – The IT Infrastructure of the Future

Second, SSC will realize its technological vision through the efforts of its six key program areas:

1) Email Transformation Initiative (ETI): The ETI was put in place to leverage a whole-of-government approach and industry expertise to establish a single enterprise email system with a standard *@canada.ca* naming convention. This system is designed to improve public access to government services and overall service quality, value, and security. Through the ETI, SSC is consolidating and modernizing the email services of 43 federal departments and agencies, representing 500,000 mailboxes in 63 separate email systems across Canada.

The completion of the ETI across the 43 departments was scheduled for March 2015 and is now projected for completion by March 2018.

2) Data Centre Consolidation (DCC): The goal of DCC is to deliver government programs and services from more than 500 data centres in 2011, to seven or fewer secure, highly reliable and interconnected enterprise data centres in the coming years. The new data centres need to have back-up capability (built-in redundancy and efficiency) so that if one system or section goes offline, data and applications can still be retrieved and government operations and services will continue to be delivered seamlessly.

3) Telecommunications Transformation Program (TTP): SSC delivers consolidated, cost-effective data, voice and conferencing services across five principal service areas: 1) wide area network (WAN) services; 2) local area network (LAN) services; 3) voice services; 4) conferencing services; and, 5) hosted contact centre services. The Government's existing IT infrastructure currently comprises a series of silo-

built networks with minimal interconnectivity. Moreover, voice services are delivered through a mix of technologies, with little standardization and varying service quality.

Through the TTP, SSC is addressing these issues by:

1) Consolidating the Government's WAN infrastructure into a single enterprise network to deliver faster, more reliable and more secure network connections, to support the growth in bandwidth demand, and to reduce the number of connections to the Internet

2) Consolidating the LAN infrastructure and enabling wireless connectivity (Wi-Fi) for 80 percent of public servants by 2020

3) Eliminating unused phone lines and migrating federal organizations from outdated and costly legacy phone systems to wireless devices and new, modern technology, including Voice-over Internet Protocol (VoIP) services

4) Standardizing videoconferencing services to deliver improved interoperability, increase end-user productivity, reduce the need for travel and associated expenses, and generally generate improved value

5) Reducing duplication and achieving economies of scale by consolidating and integrating the Government's contact centre infrastructure, including public-facing contact centres

4) Cyber and IT Security (CITS): The CITS is responsible for the development of plans, designs and operations of cyber and IT security services for the Government of Canada's IT infrastructure and for Government of Canada Secret infrastructures within SSC's mandate. SSC's role in strengthening security is paramount to: 1) delivering the Government's programs and priorities; 2) protecting the privacy of Canadians; and, 3) preserving Canada's competitive advantage, economic prosperity and national security. Canadians (individuals and businesses alike) and our allies must have confidence in the Government's ability to safeguard their personal information and sensitive data.

The CITS strategy is in alignment with broader Government of Canada IT strategies and action plans, such as the *Government of Canada Information Technology Strategic Plan 2016-2020*, Communications Security Establishment Canada's (CSE) Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information (Top 10) and Public Safety's Canada Cyber Security Strategy consultations. Priorities will be continuously informed by a number of key drivers to result in the breadth and depth of

security necessary to mitigate the risks and threats facing the Government of Canada, today and in the future.

5) Workplace Technology Devices (WTD) Initiative: Workplace technology devices are essential office IT and computing equipment. This includes office productivity tools like word processing, spreadsheet and presentation software, as well as desktop and laptop computers, printers and scanners.

The WTD Initiative pursues enterprise-wide standardization, consolidation and modernization through activities such as contract consolidation. In so doing, SSC is delivering improved value by leveraging the Government's buying power, while also enhancing services to users and strengthening the Government's security posture. Departments and agencies are responsible for workplace technology device deployment, support, and asset life-cycle management.

6) Service Management: As stated above, SSC is adopting a "service first" management and program delivery approach so that SSC is a customer-centred information technology service provider. In addition to having a whole-of-department management focus, SSC is also making service management a transformation program. Under this program, SSC has established a Service Management Strategy and has implemented service-management processes and tools, such as the Service Catalogue and service-level expectations for each of the IT services SSC is mandated to deliver. These strategies and tools are supported by account management teams that deal directly with client organizations for improved customer experience. A new information technology service management (ITSM) tool is also being put in place. Through a phased approach, the goal is to establish effective service-management practices by implementing mature ITSM processes to maximize efficiencies, to simplify workflows, and to enhance the quality of services delivered.

SSC's ability to deliver on each program will continue to depend heavily on government-wide alignment and support, particularly as its transformation initiatives compete for funding, resources and time across the enterprise. SSC is thus adopting an integrated planning approach to identify all key interdependencies, to directly address departmental readiness and capacity, and to ensure proper sequencing and horizontal coordination throughout execution to avoid transformation fatigue to the greatest extent possible. SSC will also continue to leverage the dedicated inter-departmental committees on enterprise-wide IT planning and priorities to support its efforts in this area.

Questions:

- *Has SSC designed the right plan for building a secure, reliable and efficient digital platform for delivering services to Canadians?*
- *Is SSC's objective to deliver modern, reliable, secure and cost-effective IT infrastructure services aligned with the IT transformation agenda and the future of IT and customer needs?*
- *Does SSC have the right business capacity and skill sets in place to support a revised IT Transformation Plan?*
- *Will the proposed implementation plans help us to move toward the desired goals in each area?*
    - *Do those implementation plans raise new issues that SSC will need to address?*

Leveraging the Cloud

SSC will also make intelligent use of commercial cloud services. SSC's efforts directly support the *Government of Canada Cloud Adoption Strategy* by establishing SSC as a cloud services broker and provider through the Cloud Enablement Strategy and as the intermediary for cloud computing needs, serving its federal customers alongside public-sector stakeholders at the provincial and municipal levels. In this role, SSC will challenge its customers to build the right cases for using cloud services, while serving as public stewards to ensure that services delivered always meet the Government's highest standards of security, availability and value.

Technological Transformation – Industry

Industry participation and dialogue are crucial to realizing SSC's vision and to ensuring it remains at the forefront of technological change, delivering the highest value services to its customers. For example, as part of its procurement process, SSC regularly holds "Industry Days" and one-on-one question and answer opportunities with companies during the development of Invitation to Qualify or Request for Proposals notices associated with its telecommunications, data centre and workplace technology procurements that are posted to buyandsell.gc.ca. SSC will also continue to make effective, balanced use of the private sector, alongside in-house solutions, to take advantage of new, emerging technologies and industry managed services where it delivers the best value. For example, SSC will continue to leverage the private sector in

managing and maintaining its data centres. As specialists in the field, these companies will ensure ongoing operation and maintenance of these specialized facilities, in full compliance with the Government's operational, security and privacy policies and practices.

SSC continues to engage industry via its Information Technology Infrastructure Roundtable. Having hosted 10 working sessions to date, this forum leverages the valuable role the private sector can play in transforming the Government's IT infrastructure, and enables SSC to directly solicit industry advice and guidance on its plans. SSC will also continue to apply its collaborative procurement solutions that are based on continual consultation with industry, throughout procurement, to gauge private-sector appetite and capacity, and provide opportunities for SSC to address industry concerns. SSC will continue to refine this approach to support improved communication with the vendor community, including small and medium enterprises. Collectively, this will enable SSC to improve its procurement outcomes while adopting innovative procurement approaches.

Questions:

- *What is needed for SSC and/or the Government of Canada to meet the ever-growing demand for more IT hardware, software and systems to deliver services to Canadians?*
- *Will SSC's IT Transformation Plan be adequately aligned with IT sector trends and vendor capacity?*
- *Are there industry benchmarks against which SSC can gauge the progress of its transformation?*

CONCLUSION

At the end of the day, Canadians expect secure, prompt and reliable service, delivered when and where needed and at the highest possible value. SSC remains committed to supporting the Government in meeting, if not exceeding, these expectations and, in so doing, realizing the vision of a modern, digital public service, making smart use of technology to best serve Canadians.

Notwithstanding the many challenges, the creation of SSC remains a sound government decision. The Government of Canada could not continue to operate on outdated technology, and the idea that each federal organization would modernize its IT infrastructure by building independent systems one by one is simply not viable. Government has to work together, building a shared service and IT platform and eliminating inefficient duplication in the process. In fact, the assumption of a common IT infrastructure underwrites the Government's entire digital vision; without it, this vision cannot be realized. This includes ensuring adequate cyber protection of Canada's and Canadians' data, which necessitates the establishment of a strong perimeter defence, with all organizations behind shared firewalls and IT security defences.

SSC's transformation agenda is bringing all of government together to build the IT backbone to underpin service delivery for years to come. This is not an easy task. It demands leadership, it demands perseverance, and it demands a service-oriented organization that listens to its customers, coupled with customers committed to working in partnership to realize a shared vision of IT service excellence, even in the face of challenging operational conditions. SSC is confident it can and will continue to meet these demands, armed with a more sustainable business model, a more realistic and better integrated implementation approach, and a service-first philosophy. Canadians expect and deserve no less.

Questions:

- *What three things will make SSC successful?*
- *What three things could interfere with making SSC successful?*