Digital Operations Strategic Plan: 2018-2022

Digital Operations Strategic Plan: 2018-2022

On this page

About this document and what's new

This Digital Operations Strategic Plan is the third iteration in the Government of Canada's strategic planning process for how we manage technology and technological change in government. This Strategic Plan builds on and expands on the Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021 (2017 to 2021 GC IM-IT Strategic Plan), which itself built on and expanded on the Government of Canada Information Technology Strategic Plan 2016-2020.

This Strategic Plan sets and provides insight into the government's digital direction. Departments and agencies, chief information officers (CIOs) and officials should consider it as direction from the CIO of Canada. In addition, while broader in scope, this Strategic Plan should be interpreted as the government's annual strategic plan for information management (IM) and information technology (IT) according to subsection 6.4.2 of the Policy on the Management of Information Technology. A more detailed list of Strategic Action items and related direction is included as an Appendix for ease of reference.

Unchanged from the 2017 to 2021 GC IM-IT Strategic Plan, the Strategic Plan's vision statement includes the statement that "digitally, the [Government of Canada] must operate as one to benefit all Canadians." The move from an IM-IT strategic plan to a Digital Operations Strategic Plan supports this ideal, and acknowledges the need for greater integration in government to deliver on this digital vision, including across functional communities and within teams.

This Strategic Plan establishes the integrated direction for the government on digital transformation, service delivery, security, IM and IT. It identifies cross-government priorities and key activities for departments and agencies, including those that provide services to other government organizations. It is intended to be a key input into

departmental IT planning, IM-IT investments, service improvement and digital transformation initiatives. As part of this process, departments and agencies will use this plan to internally prioritize digital investments and initiatives, and demonstrate alignment with the government's overall direction.

As in previous years, this Strategic Plan identifies priorities and activities that are required of internal enterprise service organizations such as Shared Services Canada, Public Services and Procurement Canada, and the Canada School of Public Service in order to modernize service delivery, improve sustainability and promote digital government. These initiatives will enable departments to move toward digital program and service delivery for Canadians, while also supporting individual departmental mandates and requirements.

The updates in this Strategic Plan address feedback received on previous strategic plans, and reflects consultations with senior government leaders, partners outside of government, and other levels of government from summer and fall 2018. In addition, workshops and focus groups of public servants from various departments, professional categories and levels contributed to the development of this Strategic Plan.

Message from the Chief Information Officer of Canada

Public servants across the Government of Canada are working on delivering a digital government that is more open and more collaborative, and that provides improved digital-first, user-centred services and programs.

This Strategic Plan is about charting a course to that digital government vision, and is focused on practical steps and implementation over the next 4 years. The Strategic Plan is 3 things at once: a vision, a strategy and an action plan.

This Strategic Plan builds on last year's 2017 to 2021 GC IM-IT Strategic Plan, which included draft digital principles, mentioned the development of the larger Digital Policy, and had the same ultimate vision as this Strategic Plan. This vision is:

> The Government of Canada is an open and service-oriented organization that operates and delivers programs and services to people and businesses in simple, modern and effective ways that are optimized for digital and available anytime, anywhere and from any device.
>
> Digitally, the Government of Canada must operate as one to benefit all Canadians.
>
> More detail on how we will work toward this vision and detail on its components are included in the following chapters.

In short, the plan has 6 themes that make up the integrated strategy to achieve digital government, outlined in the 6 following chapters. The first 3 are components of the target outcomes of the digital government vision:

1. **A service-oriented government** with a **user-centred** approach that puts people and their needs as the primary focus of our work. A central component of this is understanding the needs of users and building our services, programs and policies around users rather than concerns about organizations or silos.
2. **An open, collaborative and accessible government** that is accountable to Canadians, shares information with them, engages them in policy development and service co-design, and works with inclusion and accessibility in mind.
3. **A digital-first and digitally enabled government** that is available anytime, anywhere, through any service window. This does not mean "digital only," but it does mean that digital service delivery cannot be an afterthought and importantly, in-person and telephone interactions must be digitally enabled to deliver excellence in service.

The latter 3 strategic themes are foundational enablers. These are necessary components that will enable and facilitate the ultimate outcomes outlined above:

4. **Modern technology and modern information practices**, including better integration between IM-IT, policy, program and service delivery, embracing innovative and responsible use of new technologies, managing security and privacy, and being data-driven.
5. **A digitally enabled public service** with the skills, the tools, the values and the mindset public servants need to enable a digital government, to deliver digital services, and to work openly and collaboratively. Both professional development and smart recruitment will play a role in this strategic focus, with the latter presenting an opportunity to promote diversity and inclusion.
6. **Good digital governance** that ensures we have proper project oversight and strategic prioritization, and that we learn from past mistakes and build on past successes. Good governance also means we promote digital leadership, nurture communities of practice and manage succession. Governance is not only about managing risk, but also about enabling innovation and experimentation.

This is a tall order. Nevertheless, I believe that the public service, working with our partners, is up to the challenge of transforming government for the digital age. Implementing this agenda is crucial to ensuring that the Government of Canada is able to meet the needs and expectations of Canadians in the years ahead.

While the strategic goals above may sound ambitious, what you will find in the following sections are concrete, practical steps, with a focus on implementation and delivery. These are included in the discussion of each strategic theme in the following chapters and detailed in a list of strategic actions in Appendix A.

Departments, agencies, and all public servants are key partners in this digital transformation and in delivering on these strategic actions.

Progress toward achieving these strategic actions and the ultimate strategic goals will be tracked, evaluated and reported. As it evolves, this Strategic Plan will require the government to make investment choices and will be reviewed yearly to ensure it stays up to date and relevant.

Working together, we will deliver on digital government.

Alex Benay
Chief Information Officer of Canada

Introduction: change drivers and challenges

The world has undergone fundamental changes over the last 20 or 30 years and continues to face dramatic, disruptive change.

Yesterday's government was one where services were delivered by analogue means, where mail correspondence, paper applications, and waiting for responses were the norm, where government information was mostly restricted, and where people had to fit their interactions with government into office hours.

All of that has changed, and government needs to change as well.

That change has begun but is still very much a work in progress. This Digital Operations Strategic Plan is about building on those early steps and charting the path forward.

Change drivers

There are a number of factors underlying broad changes in society and technology that influence the government of today, drive transformation and impact the direction of government for the future. In order to move forward and plan for the future, it is important to understand the trends driving change.

Some of these change drivers are discussed below. These underlying change drivers and challenges were considered as part of the basis for the strategic vision, digital standards and action items identified in this plan.

Connectivity and the fading digital divide

Computers and smartphones have become ubiquitous in our society, which has enabled real-time connectivity that links people to information instantly. According to Statistics Canada, the internet usage of Canadians of all ages has risen significantly over recent years, with most Canadians now using the Internet frequently or daily.

Previously, much has been made of the gap in technology adoption between individuals of different income levels or demographics; however, evidence suggests that this gap is fading. The latest research from the United States–based Pew Research Centre in Internet and Technology shows that Internet use by lower-income individuals is now only a few percentage points behind middle and upper income households, an adoption gap that had been a two-thirds difference in 2010 and a comparative adoption rate of less than half in 2000. In fact, a recent academic study found that 94% of homeless people owned a cellphone, which social advocates have called important lifelines to services.

This constant connectivity has impacted people's expectations on the speed and availability of information and services.

Public expectations

This connectivity provided by the Internet and mobile devices has meant that the public have come to expect information to be at their fingertips, available instantly, from any device and at any time.

Moreover, services provided by the private sector have become faster, better and more responsive, from e-commerce next-day delivery to smartphone ride-hailing or 8-minute automated mortgage approvals to applications that have real-time status updates for pizza orders.

Expectations of government services are not static, and as external services become easier to use, citizens expect government services to follow. Research by Accenture into e-government in the United States suggests that citizens typically want more digital government services but are discouraged by difficulties in accessing digital information or service channels.

Successful digital firms make information easy to find and services easy to use with a relentless focus on user-based research and design, and governments need to learn from this approach. Canadians want and deserve programs and services that provide the best experience for them, when and where they need it, and in a client-centred manner. However, electronic approaches have not fully displaced traditional approaches of service delivery and, in particular, people want to be able to talk to a person when they have difficulties or questions.

In this information age, citizens also expect government to be open, transparent and responsive to their views and needs. This means we need to be transparent about sharing information and be genuinely collaborative in our approach.

The growth of data

Increased computing power, the Internet and decreasing costs of data storage have led to a near-exponential growth in the data in the digital age. This data can enable new service approaches and a level of customization of services not previously possible, such as when e-commerce companies make suggestions based on past purchases, or where countries such as the United Kingdom use data from employment records to remove the need for most income tax submissions. There is a significant potential to make people's lives simpler and easier.

At the same time, managing data is a challenge for both public sector organizations and private sector firms. A survey of digital leaders by Accenture found that 59% of public service leaders in several countries and 56% of private sector leaders thought managing data was a major challenge.

Workplace and workforce evolution

Employees, who often use smartphones and digital tools in their personal lives, expect to have modern and effective tools in the workplace to enable them to serve Canadians and work effectively. This means that tools need to be interconnected, intuitive and accessible when and where they need them, and include updated business processes to make day-to-day work efficient and add value to the efforts of public servants. The government cannot properly serve Canadians if its public service has outdated tools.

In this age of connectivity, the workplace is also changing. With access and mobile devices enabled by Wi-Fi, we are beginning to build a government workplace where many employees can disconnect from their desk and work in collaboration spaces, side by side with colleagues at other departments or even in other regions. This mobility has the potential to enable public servants to move more seamlessly from project to project, and facilitates important surge capacity to address urgent needs and changing priorities. The role of telework and telepresence has the potential to promote a more regionally diverse public service and enable interdepartmental mobility, and may be especially important for a government that is competing for scarce specialist talent and for encouraging digital interchanges with experienced workers who may not want to relocate.

Rapid technological change

New technologies and business models are rapidly entering the market and will continue to do so for the foreseeable future. Advances in machine learning and artificial intelligence will increasingly enable new products and approaches, especially when coupled with the near-exponential growth in computing power and data storage capabilities noted above. The Internet of Things and smart devices are increasing in prevalence as the declining costs of sensors make connectivity economical for more uses. Additionally, other sectors of the economy will be disrupted by transformative technologies such as additive manufacturing and 3D printing, or drones and autonomous processes.

Other challenges and opportunities

Adapting government to leverage new technologies and ways of working is the major digital challenge, and opportunity, that government faces in the coming years. While this will not be easy, incorporating new technologies and new ways of doing things will have the potential to enable government to work more efficiently and effectively while providing better, faster and more responsive services to Canadians.

Other challenges that we face include:

Aging legacy IT and infrastructure needs

In order to maintain access to quality information and data, and to continue programs and services for Canadians, there is a continued need to renew or transition the government's aging and mission-critical IT infrastructure and systems that are at risk of breaking down. The challenge of maintaining these systems and upgrading was identified in previous government IT strategic plans, and work on managing this challenge has been ongoing for some time.

Security and privacy

Cybersecurity is an important and ever-evolving aspect of any government technology strategy to ensure continuity of service and safeguard citizens' private information. Consolidating systems and programs provides many important benefits but also requires enhanced security vigilance to minimize the risks of cyberattacks. Inconsistent management of government networks and security profiles of government end-point devices (computer devices that connect to the Internet) could create further challenges for cybersecurity professionals working to defend these systems. Consolidated programs, end-to-end services and tell-us-once approaches outlined in the digital government vision also increase the importance of cybersecurity and digital privacy, since more consolidated or connected information has the potential to intensify the impacts of security breaches unless risks are effectively mitigated. On the other hand, this consolidated approach allows

for a concentrated targeting of security resources compared with the effort required to ensure that thousands of decentralized systems are continuously secure and protected against evolving threats.

The growth in digitized personal information and offering Canadians improved delivery through digital approaches need to be accompanied by measures to assure that the privacy of Canadians will be protected.

Additionally, as the government moves to an open-by-default culture, it must continue to balance openness and transparency with the requirement to protect the privacy of personal information.

Digital skills

With an evolving technology environment and a new way of doing things, the skills required of public servants and leaders will evolve as well. For example, managing the day-to-day operations of a data centre requires different skills than managing vendor and client arrangements for cloud computing and cloud data storage services. Big data analysis has the potential to improve and transform functions from service delivery to policy development to auditing, but only if public servants have the required skills in big data analytics. Likewise, as government adopts machine learning and artificial intelligence tools, skills in building, procuring, managing and evaluating such tools will be required.

This challenge is compounded by the fact that some technology skills are in short supply in society in general, as well as in the public service. This means that recruitment alone cannot resolve the government's skills needs, and that professional development, including transitional training for employees in evolving jobs, will need to play a role as well. Specific areas where there is a need for investment in skills development are identified throughout this Strategic Plan, but the government will also need to broadly embrace a "learning organization" approach of continuous development if it is to ready itself for digital government and a future full of disruptive technology.

Introduction to the path forward

Effectively addressing these changes and challenges will require new approaches. The principles articulated in the digital standards and the action items outlined in this Strategic Plan will help guide the way.

For example:

- departments and agencies, CIOs, and public servants at all levels will need to be more innovative, open and collaborative

- identifying partnerships and working with peers in other jurisdictions (provincial, territorial and municipal) with academia, with non-profits and with the private sector should be the norm
- being open by default allows public service research and evidence to be peer-reviewed by Canadians and invites collaboration
- empowering staff to experiment, innovate, iterate and continuously improve creates a public service striving to deliver better services and results for Canadians

The digital government vision

> The Government of Canada is an open and service-oriented organization that operates and delivers programs and services to people and businesses in simple, modern and effective ways that are optimized for digital and available anytime, anywhere and from any device.
>
> Digitally, the Government of Canada must operate as one to benefit all Canadians.

For the context of this Strategic Plan, digital government is defined by the following 6 themes. Three are components of the vision, and 3 are foundational enablers, not necessarily ultimate outcomes, but important intermediate, internal steps to help us achieve digital government. These themes are elaborated in the following 6 chapters.

Vision components

- **A service-oriented government**, with a **user-centred** approach that puts citizens and their needs as the primary focus of our work, using tell-us-once service approaches, integrated services, and provides real-time information to Canadians about their service applications.
- **An open, collaborative and accessible government** that is accountable to Canadians, shares information with them, engages users in policy development and service co-design, and works with inclusion and accessibility in mind.
- **A digital-first and digitally enabled government** that is available anytime, anywhere, with services and information provided through multiple windows and service channels. This does not mean "digital only," but it does mean that digital service delivery cannot be an afterthought and, importantly, in-person and telephone interactions must be digitally enabled to deliver excellence in service.

Foundational enablers

- **Modern technology, information stewardship and practices**, including better integration between IM-IT, policy, program and service delivery, embracing innovative and responsible use of new technologies, managing security and privacy, and being data-driven.
- **A digitally enabled public service** with the training, the skills, the tools, the values and the mindset needed to enable a digital government, to deliver digital services and to work openly and collaboratively.
- **Good digital governance** that ensures we have digital leadership, proper project oversight, strategic government-wide prioritization that integrates business and technology planning.

Digital standards: principles for making digital government work

In addition to the specific strategic actions identified in this Strategic Plan under each theme, achieving the digital government vision will require government to working differently.

In September 2018, the government announced a set of 10 digital standards to set the standard for how government works in the digital era and guide the development of policy, programs and services in government. Prior to being announced by the President of the Treasury Board and Minister of Digital Government, these standards were published in draft as digital principles in the 2017 to 2021 GC IM-IT Strategic Plan and were refined through consultation interdepartmentally and in the open.

These are the expected behaviours for groups designing and implementing policy, programs and services in the digital era. They are intended to guide how the government and public service work on a day-to-day basis:

- **Design with users:** Research with users to understand their needs and the problems we want to solve. Conduct ongoing testing with users to guide design and development.
- **Iterate and improve frequently:** Develop services using agile, iterative and user-centred methods. Continuously improve in response to user needs. Try new things, start small and scale up.
- **Work in the open by default:** Share evidence, research and decision-making openly. Make all non-sensitive data, information, and new code developed in delivery of services open to the outside world for sharing and reuse under an open licence.
- **Use open standards and solutions:** Leverage open standards and embrace leading practices, including the use of open source software where appropriate.

Design for services and platforms that are seamless for Canadians to use, no matter what device or channel they are using.

- **Address security and privacy risks:** Take a balanced approach to managing risk by implementing appropriate privacy and security measures. Make security measures frictionless so that they do not place a burden on users.
- **Build in accessibility from the start:** Services should meet or exceed accessibility standards. Users with distinct needs should be engaged from the outset to ensure what is delivered will work for everyone.
- **Empower staff to deliver better services:** Make sure that staff have access to the tools, training and technologies they need. Empower the team to make decisions throughout the design, building and operation of the service.
- **Be good data stewards:** Collect data from users only once and reuse wherever possible. Ensure that data is collected and held in a secure way so that it can easily be reused by others to provide services.
- **Design ethical services:** Make sure that everyone receives fair treatment. Comply with ethical guidelines in the design and use of systems that automate decision-making (such as the use of artificial intelligence).
- **Collaborate widely:** Create multidisciplinary teams with the range of skills needed to deliver a common goal. Share and collaborate in the open. Identify and create partnerships that help deliver value to users.

Chapter 1: a government with a user-centred, service orientation

A digital government is a service-oriented government, with a user-centred approach that puts the needs of people and citizens as the primary focus of our work.

This theme of the digital government vision recognizes:

- service is at the heart of what government does
- users and citizens want services to be as easy to access as possible, integrated and responsive to their needs throughout their lives and life events
- policy and programs should be designed with users

1.1 Service improvement

At the core of the digital government vision is a recognition that government services should be continuously improved.

Service excellence and improvement has been a priority for the government for some time. In 1998, the government launched the Service Improvement Initiative, which led to the creation of Service Canada as a single-window service provider for many government programs, and of the Treasury Board Policy Framework for Service Improvement in 2000. As an early digitalization initiative, this policy and the Government On-Line Initiative placed a partial emphasis on providing information about services and forms online. And from 2001 to 2005, the consulting firm Accenture ranked Canada first in its annual international survey of "e-government" service delivery. In 2014, the Framework for Service Improvement was replaced by the Treasury Board Policy on Service, which is founded on the key principle that government services are to be designed and delivered considering client needs and feedback and be progressively e-enabled. This principle and the policy's requirements have been a key driver in increasing the availability of online services in recent years, such as the application for employment insurance benefits, veteran's disability pensions, and temporary resident visas, as well as income tax return filing and the issuance of licences.

Work is currently underway on a new Digital Policy that will guide the next phase of this evolution and enable better service design and delivery for the digital era, as well as better integration between the policy directions on technology, service delivery and management. Consultations on the proposed policy are underway, and its adoption is envisioned in 2019.

Budget 2016 also announced the development of a client-first service strategy to promote service improvement and transformation, and improve the experience of Canadians and businesses dealing with government. The Government of Canada Service Strategy outlined 3 objectives:

- to design and deliver client-centric services across all channels
- to provide an online experience so easy that users would choose the digital channel
- to offer a tell-us-once experience to services

Immediate efforts focus on ten work streams impacting seniors, veterans, youth, immigrants, businesses and the broader public. Details on this initiative and targeted service improvements that have taken place or are in progress can be found in the Government of Canada Service Strategy.

Going forward

User-focused design

Departments and agencies should apply user research and user-focused service design, also known as user experience design (UX), to achieve the objectives of the Policy on Service and the Government of Canada Service Strategy to design and deliver services that consider client needs and feedback. This ensures that operations, programs and policies are designed with users' needs in mind and that services are tested in practice and not just in theory.

Departmental service design also needs to incorporate the diverse needs of Canadians from a variety of backgrounds, with a focus on accessibility, inclusion and meeting the unique needs of remote communities, new Canadians, and Indigenous peoples.

To promote the digital standard of design with users, the Treasury Board of Canada Secretariat (TBS) will work with government UX practitioners to identify and address administrative barriers to user research, provide guidance on user research practices, and encourage departments to adopt user research methods and activities as a key component of designing and building services, programs and operations.

Meaningful service standards

Service standards allow the government to make a commitment to users and citizens on the quality and timeliness of service they can reasonably expect in most cases. This provides consistency for users, who can plan around these service standards, and makes departments and programs more accountable for the services they provide. The current Treasury Board Policy on Service has a requirement that priority services have service standards and real-time reporting on the performance of services, and the Government of Canada Service Strategy has identified this as an area of continued focus. In the context of the Digital Policy, consideration is being given to expanding these requirements to cover most or all government services.

Departments must aim to have meaningful service standards and real-time performance reporting in place for priority services as soon as possible, and should consider establishing different types of service standards to monitor access, accuracy and timeliness for their full range of services.

Real-time service application statuses

Real-time service application status update systems allow users to check the status of their government applications without needing to call a hotline, visit a service statement or wait to receive an update by mail. For example, since November 2016, employment insurance applicants have been able to find their latest status using the My Service Canada Account portal. In the Policy on Service, there is a requirement for departments to develop real-time application status update systems for priority services by November

2017, and the Government of Canada Service Strategy has identified this as an area of continued focus. In the context of the Digital Policy, consideration is being given to expanding these requirements to cover most or all government services.

More work is needed to achieve this goal, and there is recognition that real-time update systems can be difficult to implement given they require changes to business processes as well as technology. Nevertheless, CIOs and departments and agencies should aim make this functionality available to users.

1.2 New approaches to service

While incremental service improvements are important, the government is also considering new approaches to service that will transform the user experience and how government delivers.

Integrated, tell-us-once approaches and end-to-end service delivery provide better services by:

- recognizing that citizens view government, and sometimes even multiple governments, as a single service provider rather than a collection of silos or separate service providers
- focusing on the needs of the "whole citizen" rather than their relationship to a specific department or program

Going forward

OneGC

Canadians are increasingly expecting a seamless, integrated and consistent experience when dealing with their government. The government is often unable to provide this desired user experience given its multiple points of contact and siloed processes.

The 2017 to 2021 GC IM-IT Strategic Plan announced that "[the Treasury Board of Canada Secretariat] will develop a new strategy to set further direction on providing a single window to Canadians for all [Government of Canada] information and services and create the conditions required to transition to a single [Government of Canada] service platform." That strategy, known as the OneGC vision, aims to not only deliver on the outcome of a single window, but also go beyond it to meet Canadians' expectations of service delivery on any platform, using any device and with any partner. In the 2017 to 2018 fiscal year, the OneGC vision began to take shape.

Whether it's digital by design (see Chapter 3), the pursuit of common services such as digital identity (see Chapter 4), or making use of emerging technologies (see subsection 4.6), the government is incorporating a wide range of approaches to achieve OneGC, the individual pieces of which are explored throughout this Strategic Plan.

Integrated, proactive and end-to-end services

Many Canadians use multiple government services and are eligible to participate in various programs. For this reason, departments and agencies should understand the linkages between their services and services provided by other departments or other governments, and should seek opportunities to integrate service delivery. An example of this integrated approach is the "birth bundle" provided by Employment and Social Development Canada in partnership with the Canada Revenue Agency and provincial and territorial governments. Instead of requiring new parents to apply separately for a birth registration, a birth certificate, a social insurance number for their new child, and the Canada Child Benefit, the integrated services allow for all of them to be completed at the same time in a tell-us-once approach.

Integration can also occur within systems. Canada Revenue Agency's My Account service lets people track their tax refunds, review or change their returns, and choose whether to receive a refund by cheque or direct deposit. Employment and Social Development Canada's My Service Canada Account is the place to update personal information for employment insurance, the Canada Pension Plan and other benefits. Benefit recipients can update their direct deposit information with either the Canada Revenue Agency or Employment and Social Development Canada, and their profiles will be updated in both places, avoiding the need for duplication and the risk of missed payments.

Integration of services also means that service providers should be prepared to make referrals or "warm hand-overs" in cases where an ineligible applicant may be able to access other program options, while respecting privacy requirements. A user-centred approach and caring for citizens and their needs as a whole means that departments also need to engage with compassion and a helping, service mindset, even when the answer to a specific application is no.

Tell-us-once approaches

Even if services are not integrated in delivery, information from a wide range of services can support better service delivery across multiple departments and programs. For example, in some countries, such as the United Kingdom, payroll information provided to the government is used to pre-populate income tax returns, meaning that many citizens never need to file a tax return. In Estonia, the government only ever asks for a particular piece of information once. For citizens and service users, this means less time filling out

government forms and fewer delays in accessing service. Implementation of a single, secure Digital Exchange Platform to allow information to be used for multiple purposes would enable more seamless services.

The 2017 to 2021 GC IM-IT Strategic Plan announced that TBS and departments would be exploring the potential of greater sharing of data in order to deliver better services while protecting privacy, and that the government was studying the feasibility of implementing "tell us once."

From 2018 to 2020, TBS and key service delivery departments will build on this initial feasibility study and undertake a horizontal review on information-sharing and privacy. This will identify barriers to information-sharing and make recommendations on how to eliminate roadblocks to tell-us-once government services while strengthening privacy oversight. This review will set the foundation for recommendations and potential policy changes in the future.

Data stewardship will be essential in achieving more integrated services or implementing tell-us-once approaches. The development of a Government of Canada data strategy roadmap identifies strategic priorities to support better use and management of data across the government, and enable improved service delivery to Canadians. Implementation of the data strategy roadmap complements this Strategic Plan and the actions it lays out. More information on this initiative is in section 4.

Chapter 2: an open, collaborative and accessible government

Digital government is most meaningful when it is open, collaborative and accessible.

An open, digital government recognizes that:

- transparency plays a critical role in public accountability
- government information and data is a public resource developed using public funds, and should therefore be accessible to the public, with only such reasonable restrictions as required for security, privacy and confidentiality
- government services and policies are tangibly improved when Canadians, stakeholders and users are actively involved in their creation
- government information and services should be accessible to and be inclusive of all Canadians

2.1 Open government

Open government is an approach to governance that focuses on transparency, accountability and citizen participation. Canadians want to know what their government is working on and be assured that government is acting responsibly and ethically on their behalf. In addition, citizens and businesses want opportunities to leverage government information and data in ways that contribute to social well-being and economic growth. This could include using government information and data to develop services, build businesses and support academic research.

Openness and transparency benefit government and Canadians alike, including by:

- supporting public accountability of government administration, including the responsible use of funds collected from taxpayers
- inviting subject matter experts and the broader public to make use of government data, research and analysis
- allowing opportunities for citizens and stakeholders to participate in the study, design and implementation of public decisions
- demonstrating that departments are using the best available information and data from a variety of authoritative sources to make evidence-based decisions with respect to policies, programs and services
- providing access to valuable government data, which can be used to develop tools and products that contribute to Canadians' well-being and economic growth

In recent years, Canada has emerged as a leading voice in the global open government community. In October 2018, Canada began its term as lead government chair of the Open Government Partnership, a multilateral initiative comprising over 75 member nations that aims to secure concrete commitments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance, in partnership with civil society and the private sector. Canada will focus its one-year chair term on open government activities that promote inclusion, impact and citizen participation, culminating in the OGP Global Summit to be hosted in Ottawa in May 2019.

Domestically, the government continues to make improvements to the Open Government Portal, open.canada.ca, an online platform hosting more than 80,000 datasets and government records from over 70 federal departments and agencies. The government has also brought forward a bill to modernize the Access to Information Act, including a strengthened role for the Information Commissioner and a legislated system for proactive publication. Further details on these and other open government initiatives are outlined below.

Going forward

As part of its Open Government Partnership membership, Canada expects to release the National Action Plan on Open Government for 2018 to 2020 in fall 2018. The draft plan includes 10 commitments on topics ranging from digital government and services to open science, reconciliation and open government. The consultation process behind this plan, conducted between October 2017 and August 2018, was the Open Government team's most ambitious outreach initiative to date, with more than 10,000 people participating through online and in-person events held in 17 cities across Canada. The plan will also be the first to incorporate expert feedback from the newly convened Multi-Stakeholder Forum on Open Government, and from 4 independent experts invited to conduct a feminist and inclusive review of the plan.

Open data

In 2018, Canada was ranked 1st place (tied with the United Kingdom) on the World Wide Web Foundation's global open data index, the Open Data Barometer. The government will build upon this success through continued improvements to the Open Government Portal.

Recent improvements have focused on simplifying the user experience for access to datasets held across different levels of government. As more Canadian provinces, territories and municipalities create their own open data portals, end users are forced to navigate between platforms to access the data they need.

To address this issue, the Government of Canada launched a pilot with provincial partners within the Government of Alberta to allow for the simultaneous search of Alberta's provincial datasets through the federal Open Government Portal. The National Action Plan on Open Government for 2018 to 2020 will include commitments to extend this federated data search pilot to 2 more provinces and 2 municipalities by 2020.

Access to information

In 1983, Canada introduced one of the world's first Access to Information regimes for the public disclosure of government information. Today, the government is working to modernize the Access to Information Act to ensure that the system is responsive to the needs of contemporary users. Additionally, a new Access to Information and Privacy Online Request Service portal was launched on October 10, 2018. This portal, designed through user testing, uses artificial intelligence to enable requesters to search for summaries of previously released Access to Information requests and to help requesters to identify which institutions would likely hold the information they seek. It also allows for electronic payments and electronic transfer of the request to federal institutions. The solution will continue to be iterated through additional user testing, and institutions will continue to be phased in until all institutions (260+) subject to the Access to Information Act and the Privacy Act are receiving requests through this service.

To reduce the administrative burden on federal institutions and to improve service to Canadians, efforts are currently underway to digitize the end-to-end access to information and personal information requests by 2021.

Open by default and proactive disclosure

The practice of releasing information of interest to Canadians proactively, rather than requiring public requests for government information, is a major cornerstone of an open government. The government has strengthened this practice in the recent amendments to the Access to Information Act and will continue to make more information proactively available.

While it is important that protected information is secured and properly categorized, departments should be careful about over-classifying information in a way that restricts Canadians' Access to Information rights or undermines the government's open-by-default approach.

The release of government research, program performance evaluation, and other information helps assure Canadians that government decisions are evidence-based. All public servants are responsible for information management, and CIOs have special responsibility for ensuring that information is properly managed through its life cycle and is available to Canadians when appropriate. CIOs should consider designating an official responsible for open-by-default and proactive disclosure.

Other initiatives, such as the launch of a Government of Canada wiki available to the public and the Open Maps portal, will also proactively provide information to Canadians.

2.2 Collaborating with Canadians

Citizens want to be consulted and their views considered as part of policy and program design, and they want access to digital tools to better participate in policy and program development.

Government consultation and collaboration help improve services and policy in a variety of ways. For example:

- new information, ideas or alternatives can be developed in these processes resulting in a better policy or service design
- consultation can identify barriers faced by service users and allows the government to consider the impacts on or different needs of diverse groups

- information gathered through consultation can help identify the issues underlying policy problems, including potentially avoiding previously unknown unintended side effects of policy
- consultation can also help identify the extent of a problem and help prioritize action

The government has made significant advances in digital collaboration in recent years. A relaunched Consulting with Canadians website provides a central portal for people to search for and respond to consultations across government. GCcollab has been launched to enable document-sharing and collaboration with stakeholders across silos and jurisdictions. In addition, government is increasingly using sites such as GitHub, Google Documents or social media to co-design elements of policy or services. This work will continue.

Going forward

Consultation and research with users must be incorporated into service and policy development, and CIOs should identify opportunities to use collaboration and co-design within product development. Rather than exclusively using government tools, the government should also leverage open platforms, such as GitHub or social media, to collaborate with Canadians and experts.

Digital consultation tools

The GCcollab tool that has enabled public servants to work collaboratively with academics, community organizations and members of the public will be relaunched and iterated in 2019, with enhanced features, more user-friendly interfaces and a more accessible sign-up system.

As announced in Budget 2018, the government is also developing a platform for regulatory consultations where respondents can comment on specific clauses of proposed regulation.

2.3 Accessibility and inclusion

A government is only truly open if it is open to all people. Accordingly, accessibility and inclusion is a key component of digital government.

Accessibility by design and inclusion by design support a government where:

- the needs of all people are reflected in the provision of government information
- views and needs of diverse Canadians are considered in government administration and consultations

Furthermore, services must be accessible by design, meeting or exceeding accessibility standards, and the testing and research to deliver excellent experiences for users must be inclusive of those with distinct needs. Users with distinct needs should be engaged from the beginning to ensure that what is delivered will work for everyone. User-centred service design (UX), as discussed in the previous chapter, can assist with this.

The government has brought forward transformative legislation, Bill C-81: An Act to Ensure a Barrier-Free Canada, also known as the Accessible Canada Act. The act seeks to help identify, remove and prevent accessibility barriers in areas under federal jurisdiction and within the government.

Going forward

Implementing the Accessible Canada Act

The government has recently created a new deputy minister position for public service accessibility and is working to remove barriers to accessing government information and services, as well as ensuring that all public service employees with disabilities have the tools and support they need to contribute to their full potential. A Public Service Accessibility Strategy and Action Plan will be released in 2019 to guide further actions in this area. This strategy and action plan will explore what guidelines, training and tools on accessibility by design are needed to ensure that the public service has the expertise and awareness to promote accessible government. The strategy will also study and recommend potential changes to government administrative policies, such as making accessibility and usability fundamental criteria in IT procurement rules beyond the use of vendor statements.

Additionally, if passed, Bill C-61 will extend accessibility requirements to government documents, expanding the requirements under current Treasury Board policies that all government websites be accessible. Departmental officials must work to incorporate the digital standard of accessibility by design into their work as a standard practice.

Inclusive communications

Under the Official Languages Act, government information is required to be accessible to Canadians in both of Canada's official languages, and departments should consider communicating in other languages, including sign languages, when user needs warrant it.

Consultation and collaboration are important components of policy-making, but these must be inclusive and accessible to identify the needs of diverse populations. Departments are responsible for consulting with Canadians and reporting on these consultations in proposals. The government is working on increasing the inclusiveness of consultations using digital tools and new techniques.

Chapter 3: digital-first and digitally enabled by design

A digital government builds digital delivery into its operations and service design, and provides the required tools to digitally enable interactions across the public service, and through all windows and service channels windows, including traditional avenues such as over the telephone or in person.

3.1 Digitally enabled by design and easy-to-find information

Going forward

Building in digital

Digital can no longer be an afterthought in operations, service design or program design. Departments are encouraged to use the digital standards as a first step in developing policy or program proposals, and central agencies are encouraged to use them as a lens when reviewing proposals or playing a challenge function. This ensures that government operations, service and program design are optimized for digital, and leverages those principles and standards, regardless of the channel through which the service is delivered.

This digital service design should build in privacy protections and accessibility by design, in line with the digital standards.

Building in privacy

Privacy must continue to be an integral consideration in the design of digital operations, programs and services; robust privacy practices and privacy breach management are foundational measures for supporting a more digital government. As the government moves toward enterprise-wide digital solutions and initiatives, for which responsibility is shared between institutions, the protection of personal information needs to be considered at the outset, through a Privacy Impact Assessment, which can identify ways to minimize privacy impacts and mitigate risks. This will support the protection of privacy for integrated and online service delivery.

Cybersecurity and information management are both important enablers that support privacy protection, and these are discussed in section 4.

Digitally enabled front-line services

While services are increasingly delivered online, human interactions will continue to be an important part of service delivery. Digitally enabling front-line services is about ensuring that the tools needed for in-person interactions between service providers and Canadians are available and accessible. The government will work to ensure that front-line services are enabled by digital tools, such as databases and telecommunications systems.

Improving content on Canada.ca

Sometimes the words we use, and how we organize them, can make it difficult for people to find and understand government information and services on Canada.ca. TBS's Digital Transformation Office is working on projects with departments to make it easier.

For each project, the Digital Transformation Office co-creates prototypes, sets concrete usability targets, and runs usability tests with Canadians, trying to improve to address specific questions that people have about specific federal services. For a prototype to launch, it must make it at least 20% easier for people to get the right answer. Considering the high numbers of visits to in-demand pages, such an increase in task success rates is significant. Ultimately, it means people spend less time looking for the answers they need from the government.

Projects undertaken in 2017 and 2018 improved Canadians' ability to find information on business start-up activities, travel documents, immunization information, employment insurance special benefits. Further information is available on the Improving content on Canada.ca web page.

Work is also taking place to improve the design system basics of the Canada.ca Content and Information Architecture Specification, with an emphasis on taking a task-based approach that prioritizes organizing online information in a way that helps people find the information or service they came to Canada.ca to find.

Departments must also use user-based research and design methodologies, as described in Chapter 1, in developing their communications.

3.2 Any-platform, any-device connectivity

Digital government involves connecting to citizens and users where they already are rather than expecting people to engage with government on its terms.

This means making government accessible on any device, through any communications channel and working with any platform.

Going forward

OneGC

The OneGC vision of interoperable systems, data-sharing and greater integration between services described in Chapter 1 will support the delivery of services on any device, any platform and working with any (trusted) partner.

In addition, the following actions also help support this vision.

Channel-agnostic services and communications

Departments should make their service and information channels technology agnostic, meaning that citizens and clients should be able to interact with the government through their preferred platform rather than being forced to use a platform preferred by departments.

For example, departments should not force clients to send information by fax or mail without compelling business reasons. Previously, student loan documents required physical signatures and needed to be mailed, but since 2015, the National Student Loans Service Centre has accepted electronic signatures and online submissions. However, consistent with the "digital first, but not digital only" approach, students still have the option of mailing documents or dropping them off in person at the financial offices of post-secondary institutions.

Better management of the government's mobile presence

Canadians and business want to use mobile options to interact with government data and obtain government services. These interfaces need to be relevant to Canadians' needs and be easy to use while respecting privacy and security requirements.

As part of the overall web strategy, it was announced in the 2017 to 2021 GC IM-IT Strategic Plan that the government will develop a strategy and framework for the development and management of mobile applications that are easy to use and trusted. Approved government mobile applications will be identified on Canada.ca and available through application stores.

However, mobile applications should be created only in appropriate circumstances when there are clear use cases. The Standard on Optimizing Websites and Applications for Mobile Devices says that "device-based mobile applications [may not be] the sole means

of providing information or service. Device-based mobile applications must be provided only to enhance information and services available through Government of Canada websites and Web applications." Among other issues, device-based mobile applications are not always accessible to all devices and users. Other service providers and governments, such as the United Kingdom's Government Digital Service, have moved away from the use of mobile apps toward web-based applications that do not require downloads and are not device-specific. Before creating a downloadable mobile application, departments must develop a clear use case and determine whether more accessible options will achieve their desired results.

Personal voice assistant compatibility

A recent technological trend that shows no sign of slowing is the prevalence of personal assistants such as Apple's Siri, Amazon's Alexa, Microsoft's Cortana and Google Assistant. These smart programs help people organize their lives: they can maintain calendars, organize shopping lists, pay bills and search for information on demand, and more. And with the pervasiveness of smartphones, such programs are becoming widely available and used. The government is working to make government information easier for personal assistants to search, so that these devices could serve as a window to access services in the future.

Consistent with the policy approach on optimizing for mobile devices described in the section above, government interfaces through personal voice assistants must be an optional information channel that complements rather than replaces other information channels for those that opt in to these third-party platforms.

Chapter 4: modern tech, technology practices and information stewardship

Canadians rely on the government for programs and services, which in turn depend on reliable, authoritative data and enabling IT capabilities to ensure successful delivery. Accordingly, processes to manage technology and information assets are key enablers of the digital government vision.

Specifically, it is important to ensure that regardless of location, Canadians have a consistent experience when interacting with the government. The design and delivery of technologically enabled services must consider latency, bandwidth, infrastructure, privacy, security and service levels.

Modern solutions are enabled by and in turn enable the use of reliable, authoritative data to inform decision-making and innovative approaches to both policy and service delivery. Data stewardship is critically important to:

- enable public servants to find, use and share these data assets over time
- ensure data security, integrity and the privacy of personal information

The government's systems and IT infrastructure are also aging. To continue providing programs and services for Canadians, it will be important to prioritize the renewal or replacement of at-risk IT infrastructure and systems.

New mechanisms such as cloud and other service delivery models are being established to improve the stability of existing systems and services, and to better balance infrastructure supply and demand. While progress has been made to rationalize applications, the government still operates more than 8,900 applications. In addition, current system health indicators signal that more work is needed to address the risks associated with aging IT.

The government must embrace the innovative and responsible use of new and emerging technologies while keeping in mind users, accessibility, security, privacy, and good data stewardship and information management requirements.

Addressing this reality requires vision, a commitment across funding, leadership and change management, a plan to deliver and, most importantly, solid execution.

CIOs and their staff have a leadership role in delivering on the digital government vision by collaborating, learning, innovating and working more strategically across established silos. It will also be important that they work in partnership with business owners in operations and program and service delivery to ensure an integrated digital government approach.

4.1 Network and infrastructure

A modern, sustainable, reliable and robust technology infrastructure enables horizontal digital service delivery, collaboration and information-sharing across government and with citizens, external business, stakeholders and partners. It is also a critical enabler of the shift to client- and service-centric program delivery and the establishment of government digital services. This includes connectivity infrastructure, which is needed to use web-based digital tools, engage with Canadians and link to cloud services, and is thus paramount to delivering on digital government. The infrastructure required for effective information stewardship, data centre operations, and connectivity to cloud systems is likewise critical to achieving this vision.

Many of the government's legacy data centres have limited capacity and are at risk due to age and the end of lease agreements. This has prompted the government to focus on a data centre consolidation strategy that advocates transitioning to a limited number of modern enterprise data centres. While the government has made progress in advancing this strategy, the government continues to operate over 500 legacy data centres, which support service delivery or business functions, including mission-critical operations.

In parallel, the IT industry has been increasingly commoditized, making it more cost-effective to treat IT services as a commodity, to be procured from and delivered as a service in cloud deployment models. In a cloud model, vendors are responsible for maintaining and renewing the infrastructure, upgrading applications, and adding new capabilities, and customers purchase computing power on demand rather than acquiring and operating the infrastructure themselves. This computing power is metered similarly to water and hydro services based on customers' rising and falling needs and is priced based on consumption. This model enables ubiquitous access to shared systems and higher-level services, all of which can be rapidly deployed with minimal effort, leading to improved coherence and economies of scale.

The trend of increasing commoditization and deployment of cloud models is certain to continue, although the rate of change from traditional to commoditized services is unknown. Given this, CIOs must continuously evaluate the "buy or build" decision, as well as re-evaluate the value of sunk costs. Budget 2018 likewise recognized this shift and provided funding to Shared Services Canada's customer departments "to help them migrate their applications from older data centres into more secure modern data centres or cloud solutions."

TBS will continue to provide policy direction and guidance to CIOs, including the cloud-first policy requirement of the Policy on Management of information Technology.

Going forward

Workload migration and cloud adoption

Given the risks posed by aging data centres, TBS and Shared Services Canada are leading a workload migration initiative, working with departments and agencies to migrate their applications from legacy data centres to new infrastructure in either enterprise data centres or cloud services. Care is always taken to ensure that both mission-critical and other applications are stored in the appropriate environments, and that applications are supported by technologies and procedures that ensure their availability.

As indicated above, the government's strategy for decommissioning legacy data centres includes 2 high-level paths: migration to enterprise data centres or to cloud services. However, this choice is not entirely binary. In making their decision, CIOs will need to consider which portion of their application portfolio is both appropriate and ready for each stream.

In addition, the cloud landscape can be generally be divided into 2 models: public cloud and private cloud models. In a public cloud model, government organizations share secure tenancy with other consumers of a cloud service, including private companies, non-profits and individuals. By contrast, a private cloud is dedicated to the needs and goals of a single organization. In this model, the government would therefore be the only tenant, provided on either vendor or government premises and managed either by a private service provider or by the government.

The Canadian market is currently well served by major public cloud service providers, who are already delivering services to the government, and public cloud services will be the priority choice for CIOs when choosing a cloud deployment model. The government faces the question of how to introduce private cloud into this landscape for use cases that cannot be served by public cloud (for example, secret information). This includes determining how to scale private cloud services, as demand may rise and fall over time. To mitigate the risk that the government over-invests in private cloud service and ensure that private cloud services are sufficiently scalable, Shared Services Canada will conduct a proof of concept designed to evaluate the scale and scope of government private cloud service requirements.

Adoption of cloud will also drive changes to the government's traditional IT model and associated roles and responsibilities, due to cloud-inherent characteristics such as:

- a high degree of automation, where policy enforcement, tasks, monitoring and access can be conducted with little human intervention
- self-service provision and configuration of services and resources from a centralized web-based console
- consolidation of the technology stack, where traditional separations between infrastructure and applications become blurred, causing an evolution from application developers to stack developers

Accordingly, adoption of cloud services delivers modernization benefits, but not without also requiring changes in governance models, risk tolerance, culture and the workforce.

CIOs will ultimately need to determine the pace at which they migrate to cloud services. For some departments, this transition will likely occur over the next few years; for others with unique business requirements and or customized systems, the transition may be

longer. Drivers behind the pace of migration include investment levels, the extent of the risks associated with aging technology and transitional disruption, organizational culture, and workforce skill sets.

In creating a cloud-first requirement in the Policy on Management of Information and Technology, the government has assessed the potential risks posed to data sovereignty, data residency, security and privacy. To ensure transparency and Canadians' continued trust, the government has published:

- a white paper on data sovereignty and public cloud
- Direction for Electronic Data Residency
- Direction on the Secure Use of Commercial Cloud Services
- Government of Canada Cloud Adoption Strategy

These detailed documents will continue to collectively guide the government's adoption of cloud. It bears noting that perhaps the most critical risk mitigation strategy that department and agencies can implement in adopting cloud is to build a cloud-savvy workforce.

For departments and agencies that migrate to the enterprise data centres, Shared Services Canada will provision and operate the platforms required to host departmental applications. TBS will also work with Shared Services Canada to establish an application hosting funding model that allows CIOs to allocate funding according to their target decision (that is, cloud services or an enterprise data centre).

Complete telecommunications and network consolidation

To streamline and modernize the government's network infrastructure and services, Shared Services Canada will eliminate unused phone lines and migrate departments from outdated and costly legacy phone systems to wireless devices and VoIP (Voice over Internet Protocol) service. Efforts will be made to consolidate customers' wide-area networks into a single enterprise network, establish shared network infrastructure in office buildings that house multiple departments, and secure and reduce the number of connections to the Internet.

Network connectivity

The government requires a diverse network landscape to deliver on its digital government vision. To begin, high-performing Internet service is required to enable citizen interactions with their government through multiple channels, as well as public servants' use of digital, telepresence and cloud-based tools. In this way, reliable and responsive networks will be the highway upon which the government's data travels.

Likewise, the availability of mobile networks and Wi-Fi will enable the federal workplace to equip itself with the same productivity tools that have become ubiquitous in public servants' personal lives. Indeed, the digital workplace increasingly includes more open, collaborative use of digital tools and the transmission of information, all of which increases network demand. Cellular networks are likewise needed to maintain employee productivity and contact with the office when travelling or working virtually. Dedicated, reliable network connections to cloud service providers are also a prerequisite to government cloud adoption at an enterprise scale, ensuring CIOs can fulfill their cloud-first policy requirement. In parallel, the government will continue to support special purpose networks such as the Government of Canada's secret network and science network.

This diverse landscape of networks will continue to evolve as data volumes increase and data locations change over time.

Enterprise-wide IT service management

IT service management refers to the planning, delivery, operation and control of IT services provided to clients. While departments and agencies have historically implemented their own tools, Shared Services Canada will procure and make available a common set of IT service management tools for departmental use. This will enable IT service management consistency across government, reduce the overall cost, and should reduce service request fulfillment times.

4.2 Secure and trusted

Canadians rely on the government to provide secure digital services in a way that protects the information they provide to the government. Canadians who use government services must have confidence that:

- any personal information they provide is stored and handled appropriately
- they are informed about how their information will be used by government
- they can access the personal information they provide
- their privacy is protected while they use the service and afterward
- the system they're using is safe and secure

"Secure and trusted" focuses on safeguarding sensitive government data, ensuring that the systems underpinning digital services are properly designed and secured, and that Canadians accessing online services can trust the government with their personal information. As the shift to digital services increases and the government modernizes its technology and IM and IT practices, it must also continue to evolve its defences. Canada's competitive advantage, its economic prosperity and its national security depend on the

government adopting new, accessible technologies to better serve and protect Canadians and public servants. If not managed well, however, making information and data more open could risk exposing networks, systems, devices and data, including personal information, to malicious or accidental breaches. This is just one reason why strengthening IT security is paramount.

The government must therefore establish a secure and resilient enterprise digital security ecosystem in which government services are delivered safely and securely. Building in privacy and security from the outset and using an information-centric approach will enable the delivery of reliable services that grant access to protected assets to trusted and verified users only. Proportionate security safeguards, based on the sensitivity and value of information, must be implemented with due consideration for ensuring minimal impact to the user. Taking a pragmatic approach to implementing security measures will help manage cyber and IT security risks and costs, and help provide a seamless and frictionless experience to the public.

Going forward

Trusted access

A trusted digital identity system is fundamental and is a key enabler of seamless and frictionless security in digital systems. TBS will continue to evolve external and internal authentication. This includes enhancing Sign-in Canada, the authentication service for external, public-facing services, so that it can accept trusted digital identities from provincial and territorial governments. To support internal government workers, TBS is working with Shared Services Canada to implement common internal identity and credential processes and technologies tailored to the level of assurance required for particular business processes. When developing digital services that require digital identity authentication, departments will make use of these common enterprise solutions to enable access to government services for authorized parties. TBS, Shared Services Canada and other departments will continue to work together to minimize the misuse, whether malicious or accidental, of any account that has elevated privileges. Sharing personnel screening information more quickly will also help reduce the risk of insider threats.

Protected assets

With the increasing sophistication and frequency of cyberattacks, the government must continue to be vigilant and strengthen its defences. By using an information-centric security model supported by a trusted digital identity, the government will have the means to protect assets (including devices and information) throughout their life cycle. Establishing a real-time, enterprise view of the current status and configuration of

government end-point devices that are authorized to use secure end-point profiles means that the government can identify end-point devices that pose a risk to the enterprise and respond to threats and attacks more effectively. Departments must ensure that systems are well maintained and administered through their life, including protecting devices and interfaces, especially those that are used for administration that are frequently targeted.

As the government adopts alternate service delivery models such as public cloud and hybrid clouds, it must continue to provide a secure, reliable and interoperable service delivery environment for internal services and business applications that are hosted in cloud–based environments. By applying a defence-in-depth, layered security approach, the government can continue to keep pace with evolving technology and practices and implement adequate safeguards to protect government information and assets. This includes establishing additional trusted interconnection points to act as a gateway to access cloud services and to protect cloud-based workloads from direct attacks from the Internet. Protecting sensitive information and preventing data loss is further supported by using secure communication tools such as the Government of Canada Secret Infrastructure, a single, common and integrated enterprise-wide secret-level network that enables secret-level classified data to be securely transmitted, stored and processed across departments.

Resilient services

Delivering secure and trusted digital services requires systems and applications to be built with resiliency against cyberattacks from the outset, as part of its design, implementation, operation and management. As the government adopts more agile and iterative processes for development, it will have to focus on security and privacy from the beginning. Doing so will help ensure that coding quality and architecture issues don't cause software security weaknesses, and reduce vulnerabilities throughout the life of a system by ensuring that patching and maintenance cycles are respected. Using secure protocols by default, such as HTTPS, will help protect the information that Canadians provide to the government through its publicly accessible websites and web services.

Continuous monitoring of the digital environment requires consideration of the cyberthreat and risk landscape, which informs decision–making and influences how the government prioritizes corrective actions across the enterprise to ensure maximum protection of assets. Consideration must also be given to how delivery of the digital service can continue in the event of technology failure or compromise. Even with the protective measures outlined above, cybersecurity events (including cyberthreats, vulnerabilities and incidents) will inevitably occur, and the government must be prepared for them. By continuously improving the <u>Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018</u>, the government's operational framework for managing

cybersecurity events, the government will be able to respond to cybersecurity events quickly, consistently and in a coordinated manner, which is essential for ensuring the sustained delivery of programs and services.

4.3 Procurement modernization

If modern technology is an essential enabler for digital government, procurement modernization is an equally essential enabler of modern technology. Governments cannot reasonably hope to have a portfolio of modern technology if procurement cycles continue to take years and deliver products that have begun to become obsolete.

Departments have been challenged by complex and time-consuming procurement policies and processes that have made it difficult acquire goods and services in a timely manner. This has been particularly true for technology-related procurements, and this procurement complexity contributes to the length and expense of projects. These difficulties with procurement undermine transformation initiatives and have operational impacts on the delivery of services to citizens and businesses.

CIOs need to be part of the solution to these procurement difficulties. The role of CIOs is evolving from that of IM-IT service providers into strategic business partners, innovation agents, business enablers and catalysts for enterprise transformation. In an integrated digital government approach, they will bring IM-IT to the table in innovative ways to address the department's business needs, support transformation initiatives, seek opportunities to partner with innovations hubs on pilots, and lead agile development of solutions.

Going forward

Procurement modernization

TBS, in partnership with Public Services and Procurement Canada and Shared Services Canada, is leading a government-wide initiative to identify and support key improvements in the federal procurement regime.

Departments should take advantage of existing multi-departmental contracts when investing in technology solutions to meet common needs; this will allow departments to implement technology needs without duplicating procurement processes. In cases where multi-departmental contracts or tools do not meet business requirements, departments will discuss other options with TBS, including agile procurement. Departments are required to keep TBS up to date on their planned procurement activities through IT investment plans.

Consideration should be given to agile development, regardless of contracting vehicle or approach. It will also be important to include accessibility by design for consideration in procurement.

Agile approaches to implementing business solutions

Where a customized or in-house solution is identified as the best option, application development teams should adopt modern and agile approaches to development to enable greater adaptability to evolutions in both business requirements and enabling technologies and, in many cases, delivery of greater value for business owners and clients. They must also take into account the increasingly complex ecosystem of interdependent software architecture, infrastructure and processes within departments and across the enterprise.

This will require a move away from our traditional Contract A / Contract B competitive procurements toward approaches that provide more flexibility for competitive dialogue and negotiation, allowing for requirements to be discussed, clarified, further defined, developed and improved before awarding a contract.

Agile procurement favours shorter contract periods with more off-ramps, with building solutions in a modular fashion that allows for change and iteration of both the requirement and the supplier, and with taking a test drive to try before we buy. In this approach, you don't pilot before you start the procurement; you pilot as a part of the procurement.

Cloud procurement

In the fall of 2017, Shared Services Canada began awarding contracts to cloud services providers qualified to host data at the unclassified level. Aligned to the relief valve strategy outlined in the Management Summary and Recommendations: Shared Services Canada Resource Alignment Review, a light-touch brokering model was launched whereby Shared Services Canada provides cloud subscriptions to departments from which they provision, manage, and operate cloud resources and services.

Shared Services Canada will continue to support a light-touch brokering model as it moves forward with procuring public cloud services qualified to host protected data.

Complementing the light-touch broker, Shared Services Canada will add optional services to accelerate public cloud adoption and reduce time to achieve compliance with the Direction on the Secure Use of Commercial Cloud Services.

One such initiative will make available reusable, self-service provisioned architectures, templates and policies for the highest-demand public cloud service providers. To accelerate this work, Shared Services Canada will leverage work completed by pathfinder departments. As indicated above, public cloud services will be the priority choice for departments when choosing a cloud deployment model.

Shared Services Canada will also complete proof of concepts for private cloud, as outlined in the IT modernization section of this document (subsection 4.4). The outcome of these proofs of concept will inform governance decisions regarding the brokering of private cloud services at the Government of Canada Enterprise Architecture Review Board. Departments will use private clouds where needs cannot be met by public clouds (for example, secret information).

Software as a service (SaaS)

As with other cloud services, the SaaS market trend is a potentially disruptive way of doing business and has many benefits. This approach allows software products to be acquired not as a one-time purchase but rather as an ongoing service. This approach:

- reduces up-front costs and instead introduces ongoing subscription costs
- keeps the product evergreen, with ongoing updates and evolutions to address emerging requirements, which reduces maintenance costs, eliminates upgrade costs and avoids long-term legacy issues
- eliminates disincentives for organizations to update to newer software versions

Public Services and Procurement Canada will undertake activities to create a source of supply for a wide range of SaaS products.

SaaS should be a CIO's priority choice when choosing a cloud service model. Hosting software in the cloud or managed services can often be misrepresented as SaaS. While these are legitimate service models, they do not maximize the benefit the government seeks from SaaS. To ensure SaaS benefits are realized, CIOs need to look for these characteristics:

Characteristic	Benefits
Subscriptions, not licences	Subscriptions remove the need for the government to patch and fix software, as this is left to the service provider (improves security and performance).
The government is one client/tenant among many	The supplier will continue to make improvements to remain competitive and attract new tenants.

Professional development in support of procurement modernization

As noted elsewhere in this Strategic Plan, departments need to promote a learning culture to help enable digital government transformation. For procurement modernization, this means supporting solutions architects and developers to:

- understand and adopt agile practices, including iterative development approaches, automate release schedules, and embrace a layered testing strategy, including automated testing
- develop the engagement and collaboration competencies needed to advance iterative approaches and engage functional experts, program managers and users early in the development process
- support the professional development needed to deliver on the cloud-first approach and increase the use of SaaS

4.4 IT Modernization

As noted in subsection 4.1, a modern, sustainable, reliable and robust technology infrastructure enables horizontal digital service delivery, collaboration and information-sharing across government and with citizens, external business, stakeholders and partners. It is also a critical enabler of the shift to client- and service-centric program delivery and the establishment of government digital services.

A number of IT modernization initiatives are underway that support the transition to digital government and that reflect the new role of the Office of the Chief Information Officer of Canada and the roles of TBS, Shared Services Canada, Public Services and Procurement Canada, and other partner departments in this new paradigm.

Going forward

Government email solutions

Departments have traditionally operated their own email systems, resulting in business and cost inefficiencies. Shared Services Canada as the service provider and TBS as the enterprise business owner are developing a strategy for next-generation email services for the government.

Direction is being established to leverage the opportunity to procure a larger suite of communications tools for the government, including email services. To align with this direction, the current suite of GCTools will evolve into an open and accessible digital workspace, discussed in subsection 5.1.

Interoperability

A platform for government-wide interoperability will lay the foundation for achieving the data-sharing vision of getting the right information to the right people at the right time while respecting privacy requirements. This will be critically important for the successful implementation of tell-us-once approaches and integrated services, as discussed in Chapter 1.

TBS will continue to work with departments and partners on building a digital exchange platform and providing a digital exchange toolkit that includes a suite of modern integration tools (for example, identity management and data transfer systems). This toolkit will serve the needs of a digital exchange ecosystem and enable the secure exchange of data between centralized systems, departments, governments and the public.

The capability to link internal departmental information with solutions for delivering programs and services will enable greater government-wide collaboration when designing digital services, while respecting privacy requirements. It will also enable business process improvement within the government and across jurisdictions, leading to improved program and service delivery for citizens and businesses.

Through the creation and use of a governance framework (policies, directives, guidelines and open standards) for the digital exchange ecosystem, TBS will:

- foster openness and collaboration
- promote digital services
- advance enterprise interoperability and information-sharing across the government
- ensure that privacy is respected

Introduce a strategy for use of open source software and open standards

The use of open standards ensures interoperability between products and systems, and maintains flexibility within the IM-IT environment. Similarly, the use of open source software supports interoperability and information-sharing, and should be considered in the assessment of IM-IT solutions. Open source products are publicly available, and the availability of their source code promotes open and collaborative development around their specifications.

TBS will lead the development of a strategy to set direction for the government on the use and release of open source software and open standards that will be ratified using the Government of Canada Enterprise Architecture Review process.

Develop an Application Programming Interface (API) strategy

An API is a structured set of computerized protocols, automated processes and tools for building software applications, which makes it easier to develop programs by providing pre-constructed building blocks. APIs provide digital capabilities, and since they can be combined and reused to create digital services, APIs are increasingly becoming the way to facilitate sharing of government data and information. As such, they are foundational building blocks that support the government's commitment to digital government.

TBS will develop an API strategy for the government to help make the development of programs and digital services quicker and more cost-effective.

4.5 IM modernization and data stewardship

The volume of data that governments, businesses and Canadians produce is growing exponentially, driven by digital technologies. Organizations are changing their business models, building new expertise, and devising new ways of managing and unlocking the value of their data. Governments need to evolve rapidly to keep up and work in an integrated way to use data as a strategic asset that contributes to better operations, programs and service delivery.

Canadians value a government that is open with respect to data and other business information but balances openness with protection of their privacy. It is also important that recipients of services are confident that authoritative sources are used and decision-making is evidence-based.

Going forward

Developing and implementing a Government of Canada data strategy

How the government collects, manages and governs data, and accesses and shares data with other governments, sectors and Canadians, must change. Data has the power to enable the government to make better decisions, design better programs and deliver more effective services. However, we must refresh our approach for this to occur, and share data in a way that allows other governments, businesses, researchers and the not-for-profit sector to also extract value from data.

Under direction from the Clerk of the Privy Council, TBS has been co-leading the development of a Data Strategy Roadmap with the Privy Council Office and Statistics Canada since January 2018, working with other departmental partners. The roadmap identifies strategic priorities for a unified and collaborative approach to manage

government-wide data as an asset while respecting privacy. Implementation of the Data Strategy Roadmap aims to support improved decision-making and enhanced services to Canadians and a more transparent, collaborative and digitally enabled public service.

Recommendations in the roadmap are oriented around 4 themes:

- stronger leadership and governance
- improved data literacy and skills
- enabling infrastructure and legislation
- treatment of data as a strategic asset

The goal is to set a foundation so that the government creates more value for Canadians from the data we hold while ensuring the privacy and protection of personal information. Given the importance of data to supporting a digital government vision, the initiatives in the Data Strategy Roadmap complement, may overlap with, and are in some cases identical to the priorities identified in this Strategic Plan.

Data and information-sharing

When paired with modern integration tools to enable exchange of data and information between enterprise systems as well as between departments and governments, interoperable platforms are the backbone of data and information-sharing, data analytics and end-to-end services. Investments in interoperability will enable a modern workplace in which employees have the tools and data needed to keep pace with the expectations of the Canadians and businesses they serve. Seamless exchange of data and information, regardless of the underlying technology, will improve data integrity, enable the tell-me-once principle, and lead to improved operations, programs and service delivery.

As noted in subsection 1.2, changes to the rules framework may be needed to enable greater sharing of data between organizations or departments while also strengthening privacy protection in the digital age. This type of information interoperability will be a critical enabler for tell-us-once approaches and seamless services.

Ensure the quality and maintenance of data

To maximize the value and strategic use of data, dimensions of quality such as accuracy, timeliness, relevance, accessibility, interpretability and coherence according to intended use must be applied. Statistics Canada, for which data quality management and quality control are core business activities, and TBS, which supports the development of administrative policies for the government, in coordination with other organizations, will develop, implement and support data quality management strategies, policies and

practices for a comprehensive data quality framework. The proposed framework will be adaptable across government while establishing common enterprise-wide standards to ensure interoperability.

Maintain digital information

Digital assets have a longer shelf life than their supporting technologies and can be vulnerable to degradation, corruption or loss. A government digital preservation working group established by Library and Archives Canada shares common challenges and works toward facilitating long-term retention of digital assets. The work of this committee will be leveraged and expanded to develop guidance, including best practices and standards.

Enhanced open government infrastructure

As noted in Chapter 2, Canada has made significant progress in maximizing the release of government data and information. This is enabled by technology, and the government has taken important steps to improve the functionality and reliability of online infrastructure for open government.

The government has also worked to support the "demand side" of open data and information, identifying and collaborating with stakeholders in organizations and companies that leverage open government data and information. Canada's Open Data Exchange (ODX) is one organization that helps Canadian companies make use of open data. TBS has worked with ODX to deepen insight into the commercial open data landscape and to understand what challenges need to be overcome in order to make Canadian open data companies more competitive. In the last two years, ODX has incubated 15 new data-driven companies, and it has more work planned in future years to continue to promote the use of open government data among Canadian companies.

Develop a master data management program

In an open and distributed operational environment, there is a risk that business-critical data becomes redundant, inconsistent and scattered throughout the enterprise.

Master data management is the processes, governance, tools, rules and technology required to create and maintain consistent data formats across organizations and over time. It focuses on common critical data elements and establishes strong governance around them. Effective master data management can:

- eliminate redundancy and inconsistency of data and ensure its quality and control
- provide a single, authoritative point of reference that can be shared by many processes and applications across the organization
- streamline data-sharing and facilitate interoperability

TBS will work with key business owners, starting with Statistics Canada, to establish a government-wide master data management program to formally identify standard data elements and single authoritative sources for key information domains.

4.6 Innovative and responsible use of new technologies

Delivering the digital government vision will also require the government to use new technologies in innovative but responsible ways. This means following the digital standards of iterating, improving frequently and designing ethical services.

Responsible use also involves being careful about when and how new technologies and approaches are adopted but without becoming paralyzed by risk aversion. While there is a critical need to embrace new technologies to enable better, faster digital services, government cannot always be "first movers" on implementing new technologies. Sometimes, government should aspire to a "fast follower" strategy, where it monitors technological developments, evaluates new approaches, and implements them as they begin to mature and have demonstrated results. In the best cases, this can position government as an "early adopter" but not necessarily one of the very first adopters.

As new approaches are implemented, the use of pilots and iteration will be key to adapting government operations to these new approaches and manage risks.

Going forward

Responsible use of artificial intelligence and automation

Automation has the potential to a transformative force in government and to be a "force multiplier" that enables the government to provide services faster, better and more efficiently. The strategic use of automation can free up scarce resources to focus on needs elsewhere. The government announced in July 2017 that it would be running select pilot projects on the use of artificial intelligence, machine learning and automation in public administration.

The use of automation and artificial intelligence also requires careful attention to the issues of potential bias, impacts on diverse populations, risk, and managing compatibility with administrative law. To begin to identify and navigate these issues, TBS developed a working paper on the responsible use of artificial intelligence in the Government of Canada using an open-by-default and collaborative approach that engaged experts, industry professionals and the public. Work is now ongoing in developing a Directive on Automated Decision-Making and an Algorithmic Impact Assessment to provide an assessment framework that helps institutions better understand and mitigate the risks associated with

automated decision-making systems by providing the appropriate governance, oversight and reporting, and audit requirements. The tool is being developed with open collaboration.

As more use cases of automation and artificial intelligence are explored and adoption advances, more policy guidance, tools and training will be developed to help ensure that departments and public servants are using this technology in innovative and responsible ways.

Blockchain pilots

Blockchain, or the distributed ledger, is the underlying technology behind crypto-currencies such as Bitcoin. It involves storing information in distributed leaderless locations, continuously reconciling that information with the rest of the network. This application may have potential for addressing data integrity issues, reconciling systems automatically, and enabling automated trusted transactions, among other uses.

Blockchain use cases and the practicality of blockchain-based applications are still being explored by governments around the world. The government announced in July 2017 the intention to run at least 6 select pilot projects on the use of blockchain.

Chapter 5: a digitally enabled public service

Public servants are key to everything the government does: the services it delivers, the policies it develops, and the transformation initiatives within government. None of what government does would be possible without the work of public servants.

Public servants enable digital government.

To be successful, digital government must help digitally enable public servants to ensure they have the tools and the skills they need. Recruitment excellence helps play a role in enabling the public service overall.

This vision recognizes that:

- public servants are more effective at delivering services, programs and policies when they have modern tools that help their work and a modern workplace
- public servants need professional development that keeps up with changing times and changing technology
- recruitment and retention excellence plays a critical role in achieving public service excellence by ensuring that the public service has access to top talent and important technical skills

In addition, a digital public service needs to work across silos and build multidisciplinary teams, consistent with the digital standards.

5.1 Giving public servants the tools they need

Technology and tools are a force multiplier for the public service. They allow public servants to more effectively, efficiently and economically deliver on the digital government vision and government services.

This also includes tools that effectively enable public servants to collaborate across regions and departments in an integrated, seamless way to deliver the best results for Canadians. Digital workplace technologies also support other ways of working, such as the pilot project on co-working and Canada's Free Agents program.

Going forward

Workplace devices and connectivity

Workplace technology devices are essential for a modern workplace and a collaborative, mobile workforce, as also outlined in the Blueprint 2020 vision. The Government of Canada encourages an open and collaborative work environment where mobile devices are used. Mobile workstations allow employees to bring devices to meetings or collaboration spaces, and de-tether workers from their desks. For those who require being in frequent communication, smartphones allow public servants to keep apprised of developments and communications even when they are not at their desk or looking at a tablet or laptop. These mobile devices can also enable public servants to telecommute and work while on official travel. Work will continue to support the full adoption of these tools and ensure that they are reliable.

Wi-Fi service is essential for effective workplace mobility and has other benefits, such as improved employee productivity and potentially decreased infrastructure costs, compared with wireline installation. Wi-Fi adaption activities and priorities identified in the 2017 to 2021 GC IM-IT Strategic Plan will continue.

The 2017 to 2021 GC IM-IT Strategic Plan also announced that TBS will develop a mobility strategy, focusing initially on smartphones. Departments should ensure that workplace technology devices meet the Blueprint 2020 vision and promote mobility.

Teleworking

Mobile workplace technology devices can enable telework or virtual work for public servants for whom remote working is desirable and an option in their role. Virtual work involves working from various locations, which could include home in some cases, other regions or offices. Virtual work provides flexibility for workers, but can also enable public servants to work across regions and allow the public service to draw on people who are not located in the same region as a physical office location and who do not want to relocate. To enable virtual work when appropriate, departments should ensure that they have secure remote access infrastructure and procedures in place.

Video-conferencing

Increased access to video-conferencing supports the collaborative operations of virtual teams across departments, time zones and regions, and collaboration between different departments or governments.

Departments are currently working to re-engineer in-house video-conferencing facilities to enable full interconnectivity across the government, as previously identified as a priority, and Shared Services Canada will also work on enabling video-conferencing at desktops when needed.

Collaboration tools

GCTools such as GCpedia, GCconnex, GCcollab, instant messaging and the GCintranet increase productivity and enable collaboration across the government and other partners. Employees are able to easily connect and share information and work across departments and geographic boundaries, resulting in better service to Canadians.

GCTools that support government requirements for accessibility, official languages and collaboration with external partners will be further developed and integrated into other applications. The current suite of GCTools will evolve into an open and accessible digital workspace, which will allow employees to easily connect with the information, colleagues and external partners they need to work effectively. The open and accessible digital workspace will also provide simplified access to other activities such as staffing, learning and professional development.

In line with the digital standards, departments should make collaboration and appropriate information-sharing an open-by-default expectation of employees. Therefore, the adoption of GCTools should be part of standard practices for employee onboarding throughout government.

In addition, in July 2018, TBS directed departments to allow employee access to collaboration sites such as Google Docs, Trello and Slack.

Data analysis and visualization tools

As we embrace a more data-driven digital government, public servants will need access to data analysis and visualization tools. In data-driven roles, such as data scientists or policy development involving statistics, access to these tools is a basic part of the software toolkit, similar to a word processor. CIOs should make it a priority to facilitate access to data analysis and visualization tools to public servants in their departments.

5.2 Giving public servants the skills they need

To effectively deliver digital government, public servants need to develop digital skills and a service mindset. Professional development plays a critical role in allowing public servants to develop new skills, refresh their existing skills, or upskill for new, evolving requirements.

In an age of fast-moving and ubiquitous change, it has never been more important to invest in sharpening and updating skills.

Going forward

Assessing public service skills and analyzing future needs

Technological disruption, changing approaches and digital government will require public servants to have new skills and competencies. To help public servants and the public service adapt to this evolving digital environment, TBS will work with partners such as the Canadian School of Public Service to identify competencies for the digital age to better understand how the current skills profile of the government needs to evolve.

Building a Digital Academy and promoting public service digital literacy

To effectively enable digital government, the public service must promote digital literacy among all public servants. Digital literacy goes beyond basic computer skills, and public servants need to be able to use various technologies to extract high-value insights from the wealth of available information and data, use collaboration tools, and communicate in digital spaces.

The Government of Canada is launching a Digital Academy with the goal of increasing the offerings available to public servants who want to increase their digital literacy and understanding of key areas such as service design, data analytics and new technologies as they apply to their work. Informed by examples in other jurisdictions, we will build a made-in-Canada model that will lead to better understanding of how digital can improve how government functions and allow better services. The Canada School of Public Service

will lead the delivery of the Digital Academy, in partnership with TBS, the Canadian Digital Service, Statistics Canada, other government departments and partners in the non-profit, academic or private sectors.

The development of the Digital Academy will be especially guided by the principles of open by default, collaborating wisely, and iterative development. Initial courses were piloted in September 2018, and the government will aim for this service to be available beginning in 2019.

In addition to broad digital literacy initiatives, the 2017 to 2021 GC IM-IT Strategic Plan announced that the government would design an engagement and awareness program for all public servants to enable them to become more data-literate and learn the required competencies for evidence-based decision-making.

To help public servants enable a digital government, departments need to also make professional development a priority, including by ensuring that employees have the opportunity to participate in learning and development opportunities.

Enabling career development for evolving technology needs

In an age of technological transformation and disruption, professional development will ensure that technology professionals in the government are able to keep up with evolving requirements, new technologies and new approaches. In some cases, this may mean that the government helps enable IM-IT professionals to evolve into new roles and functions to serve evolving needs. For example, the use of cloud services and SaaS will require greater competencies in vendor and client relationship management, collaboration, influencing and strategic thinking, compared with a "build it ourselves" approach.

Departments are responsible for identifying public servants in positions with evolving competency requirements and for their coaching and career development. CIOs should ensure that talent managers are available to support employees that require re-skilling or upskilling to adapt to evolving IM-IT approaches. TBS, in conjunction with the Canada School of Public Service, will support this work with a career management portal and learning provider solutions.

Targeted talent management and professional development initiatives

The government is continuously evolving its approach to talent management and is expanding the scope of the program to become more inclusive to increase mobility and ensure a more porous boundary with other sectors.

Some competencies are so fundamental to effectively delivering digital government that special initiatives may be required. Cybersecurity is one of those special areas of focus, and TBS will work with developments to develop a Cybersecurity Talent Strategy. Other identified areas of special focus are data science, agile procurement competencies, and complex project management and approaches to address needs in these areas will be evaluated.

In addition, mobility opportunities can play an important role in supporting greater integration within government for better delivery. For example, the Government of Canada Policy Community has developed a cross-functional policy mobility program to allow policy practitioners in one area (for example, policy development, service management and operations) to learn about and gain experience in other functional specialities using a "learning by doing" approach. The prototype of this initiative begins its testing in November 2018.

5.3 Recruitment

Professional development alone cannot ensure that the public service is fully able to enable a more digital government. Recruitment also plays an important role for short-term surge capacity and long-term development of our future workforce.

In the context of an aging and retiring workforce, diverse and inclusive work environments must welcome intergenerational collaboration from boomers, Generation X, millennials and Generation Z. New practices and technologies taught in post-secondary institutions allow recruits to bring diverse perspectives to their teams and reinvigorate the public service through a continuous stream of new ideas. Recruitment can also allow the government to focus on ensuring a representative workforce and diverse public service. It is important for the public service to recruit and develop new talented public servants and ensure that the workforce is developed to meet the needs of digital government.

Effective recruitment also requires cyclical talent management and retention to be successful.

Going forward

Strengthening technology recruitment

As announced in last year's IM-IT Strategic Plan, the government is strengthening recruitment of technology workers through a number of initiatives. Recruitment campaigns for Computer Systems (CS) candidates led by the Public Service Commission of Canada (PSC), with educational institution partners, establishes CS inventories (lists of partially

screened candidates) from which managers across the government can hire. In addition, PSC leads timely and targeted student recruitment through the Federal Student Work Experience Program and Co-op programs that are used by departments across the government. These work-integrated learning opportunities allow students to bring in new ideas and become part of a feeder pool of candidates that have Government of Canada knowledge and experience.

Departments should consider the power of leveraging a strengthened enterprise approach to recruiting technology workers including strengthening on-site recruitment campaigns, implementing lessons learned across functional community leads, and fostering best practices in recruitment.

In addition, PSC and TBS the will work with communities to begin to explore how framing educational requirements for the CS workforce could recognize the use of alternative education or experience. Many technology firms in Canada, Silicon Valley and elsewhere have eliminated degree requirements as a recognition that the relevance of formal technology education may be outstripped by pace of technology change, and therefore, credentials, certifications or demonstrations of skills may be equally valid assessments of potential candidates.

Agile staffing

In the face of increasingly complex and rapidly evolving challenges, public servants have to work across silos, bring in new skills and capabilities, and adopt a more horizontal, fast-paced working style.

Recruitment efforts need to adapt to this reality and look to solutions beyond traditional methods. Departments should explore news ways to attract and recruit post-secondary and mid-career talent. Leading practices from the private sector such as employee referral programs and talent scouts could recruit passive candidates. To build a responsive workforce and complement recruitment efforts, initiatives such as the Government of Canada's Free Agents program and new platforms such as Talent Cloud could create a thriving project marketplace and promote opportunities to bridge short-term gaps. This is balanced with long-term sustainable investments to meet the needs of all participants in the recruitment and staffing process to accommodate the full array of identities, abilities, backgrounds, cultures, skills, perspectives and experiences in Canada's population.

There is no better way to attract talented technology workers than to showcase modern, accessible and streamlined technological features in the recruitment process. PSC will pursue further exploration and advancements in e-screening, e-testing, and remote supervised testing while leveraging augmented intelligence, among other emerging areas, to position the Government of Canada as a competitive recruiter. PSC will transform the

GC Jobs platform through agile development for a user-centric, inclusive, digital recruitment solution that will be continuously improved. The scalable solution will be key to modernizing the recruitment process that will help build the public service of the future.

Talent Cloud recruitment platform

Talent Cloud aims to build on this approach by creating a thriving marketplace where today's talent can find exciting, high-quality job opportunities that fit their passions and talents. This grassroots pilot project includes an experimental new staffing platform for project-based employment, utilizing some of the practices and advantages of the gig economy but avoiding its precariousness. The platform will launch as a working pilot in fall 2018.

Digital interchanges

The Government of Canada uses interchanges to enable transfers to and from external organizations, such as other governments, non-governmental organizations and private companies, for up to 2 years. Modelling after the approach of organizations such as Code for America and 18F, the Canadian Digital Service has utilized this recruitment mechanism to attract high-quality candidates from technology firms for a "term of service" in government, allowing the government to gain access to top tech talent while enabling technology workers to give back to government and society.

Departments should consider utilizing this mechanism to bring in talented technology workers who might want government experience but not a full career in government.

Promoting diversity and women in tech

An inclusive workplace is one where the workforce reflects the full breadth of the talent pool. Diverse teams bring broader perspectives and ideas for greater capacity to find creative solutions and innovate.

The government is committed to achieving greater representation and a balanced and diverse workforce; however, government IT remains a predominantly male domain. To address this gap, departments should proactively promote technology opportunities to under-represented groups. Further, the 2017 to 2021 GC IM-IT Strategic Plan announced that departments will develop partnerships with organizations that encourage technology as a career choice for young women, and work to encourage women leaders in the public service and the private sector to consider roles in the government's IT community.

Chapter 6: good digital governance

Governance will play a fundamentally important role in realizing the digital government vision by helping to steer the initiatives identified in this Strategic Plan. This governance will take many forms, often in conjunction with each other. Leaders and managers will play an important role in achieving specific organizational missions and in contributing to digital government within their own mandates. At a broader level, government-wide oversight and management processes will establish priorities and governance at scale, which is critical for an organization as large and disperse as the Government of Canada.

As we transition to a digital government, enterprise governance should also be enhanced and integrated to ensure that decision-making takes into consideration business needs alongside technological and information considerations, starting at conception through to delivery and beyond.

Finally, in an evolving digital ecosystem, we must acknowledge the criticality of collaboration to our success, including in developing multi-jurisdictional standards, coordinating actions, and sharing successful practices or tools. Canada will continue to play a leadership role in promoting digital government and Open Government globally, while also engaging our partners at all levels and in all jurisdictions to learn from their experiences and leverage a "build once, use often" approach.

6.1 Digital leaders

If the government is to successfully deliver on its digital government vision, it needs to foster transformative digital leadership throughout its ranks.

Going forward

CIO leadership and succession planning

The role of departmental CIOs is evolving from IM-IT service providers into strategic business partners, innovation agents, business enablers and catalysts for enterprise transformation.

To support the work that CIOs do, TBS will undertake a number of initiatives, including:

- Refresh the CIO suite of human resources documents, including generic work descriptions and competency profiles, to reflect changing technology, new IM-IT approaches, and the evolving role of CIOs. These documents will help create clear expectations for CIOs and their role within organizations, as well as simplify staffing processes.
- Strengthen talent management reviews for CIOs to ensure that digital leaders have clear expectations and are meeting or exceeding them.

- Support CIO succession planning, including identifying high-performing executives with an interest and the potential to assume technology leadership roles.
- Run a whole-of-government external competition to identify diverse CIO candidates in the private sector who are interested in government roles.

Recognizing upcoming digital leaders

Creating a public service that delivers a digital government of tomorrow will also require supporting and developing the leaders of tomorrow. It is important that departments prioritize identifying high-performing employees that demonstrate leadership qualities, embrace the digital mindset and standards, and have the potential to grow into formal management roles.

Promoting the digital leadership mindset

In addition to supporting CIOs and digital leaders in taking a more active integrated role in departmental business (for example, operations, service delivery and programs), it is important to promote the digital mindset and encourage officials working in this area to play a leadership role across their organizations. Professional development for leaders will be a key part of this. For example, the Digital Academy recently piloted a course on Agile for Leaders. Change management is likewise a skill that technology executives and workers will increasingly need, and the government will need to support this development.

6.2 Management of digital investments and results

A key component of good governance is proper oversight, approvals and performance measurement at an organizational and whole-of-government level. Strong product and project oversight and government-as-a-whole performance measurement help ensure that the digital government vision is integrated into departmental programs, services and operations. Likewise, performance measurement is essential to organizational learning and development as well as good governance, and supports proper stewardship, public accountability and transparency. It is an iterative process that must be repeated regularly.

To this end, an integrated digital performance measurement framework can lead to a set of best practices and lessons learned that can be leveraged for continuous improvement across government programs, services and operations. This includes ensuring that the digital government vision is incorporated from conception and throughout project and product development. In addition, the oversight function is critical to formal investment prioritization, and clear and consistent performance measurement reports can provide important information and guidance to government organizations on how they are progressing toward digital.

Additionally, the 2017 GC IM-IT Strategic Plan identified establishing IM-IT governance and developing methods to prioritize investments. Those actions were completed with the creation of Government of Canada Enterprise Architecture Review Board and a more formal process for prioritizing investments; however, continuing this work will be an ongoing activity and will provide important organizational leadership and governance of digital within government.

Going forward

Developing a Digital Performance Measurement Framework and Maturity Model

To measure progress on digital transformation, a performance measurement framework will be developed to accompany the Digital Policy referenced in Chapter 1. The objectives of the framework are to:

- align the Digital Policy outcomes and Digital Operations Strategic Plan priorities with discrete performance metrics
- assess the integration of digital into service delivery, operations and programs
- assess the use of performance data to support decision-making
- monitor and report on progress
- highlight achievements

A maturity model will accompany this framework to assess departments on digital government adoption, mapped to the themes included in this Strategic Plan. The benefit of a maturity model compared with more traditional yes/no compliance measurement is that it recognizes that adoption of the digital government vision involves evolution and progressive improvements. The maturity model approach also gives the opportunity to identify departments that are government digital change leaders and exceeding baseline expectations.

Data and insights generated from this process will support a continuous improvement process to inform evolving digital priorities or identify potential barriers to progress toward digital government that should be addressed.

Reviewing and updating government-wide governance committees

To ensure that our whole-of-government governance approach is appropriate to the needs of a digital government, TBS will be reviewing and updating enterprise governance, including committee mandates and memberships.

Introducing stronger concept phase reviews

TBS will enhance and strengthen the governance function for IT-enabled projects by introducing earlier reviews of investment concept cases. Such reviews will take place prior to defining the solution, allowing for early engagement on the direction. This initiative aims to:

- ensure we learn from past failures and successes
- identify opportunities for synergies or collaboration between initiatives
- maximize value and reduce operational / service delivery costs
- enable the government to respond more rapidly to emerging issues

The digital standards detailed in the introduction of this Strategic Plan will also be used as a lens to evaluate projects, products and policy proposals to ensure alignment with the digital government vision.

Enhancing digital governance and management

TBS and departments are also taking a number of measures to enhance overall digital governance, including:

- developing enterprise architectures to manage the integration business, information, applications, technology, privacy and security
- providing policy guidance and more robust approval and oversight of complex technology projects
- standardizing metadata with a registry, developing a valuation framework for information and data assets, and implementing better performance measurement for information and data management as part of the Digital Policy
- developing new business and financial models for internal enterprise service departments, with cost recovery being developed for some Shared Services Canada and Public Services and Procurement Canada services to help balance supply and demand, as announced in the 2017 to 2021 GC IM-IT Strategic Plan.
- modernizing the financial and materiel management business model across the Government of Canada.

6.3 Leadership in the digital ecosystem

A digital government in Canada recognizes the leadership role that federal government can play in spreading digital government ideas, convening partnerships, and sharing successful approaches and innovations between jurisdictions.

Canada has a long history of leading by example and participation in inter-jurisdictional forums, which the Digital Operations Strategic Plan continues and builds from.

Going forward

Leadership within Canada

The federal government plays a leadership role in promoting digital within Canada in a number of ways:

- Canada has committed to share its successes, including technologies developed by the government, with other governments and partners. For example, the Canadian Digital Service recently developed a challenge platform for the federal government and shared the technology with municipal governments. Going forward, this type of leadership will be formalized in the creation of an application and programs store (API store and App store), with Government of Canada technologies being made available to provinces and municipalities.
- In 2017, the CIO Strategy Council was established as forum for public-private dialogue on technology and digital issues with the Chief Information Office of Canada serving as co-chair. The forum involves Canada's "most forward-thinking Chief Information Officers to focus on collectively transforming, shaping, and influencing the Canadian information and technology ecosystem."

Leadership in the global digital government movement

In 2018, Canada signed the Digital 7 (D7) charter, joining leading digital nations in a mission to harness digital technology to the benefit of citizens. D7 comprises nations that are recognized as having the most advanced digital governments globally (in November 2018, it will become the Digital 9). It provides a forum for member nations to share best practices, identify how to improve service delivery to citizens, collaborate on common projects, and support and champion their respective growing digital economies. The D9 charter commits Canada to working toward core principles of digital development, with a focus on user needs, open government, and a commitment to share and learn from D9 member nations.

The Government of Canada will continue to work with Estonia and other D9 partner countries to advance mutual digital government priorities, share efforts and co-create where possible. A number of D9 working groups are being organized to address key digital issues including digital rights, digital identity, artificial intelligence and integrated citizen centric services.

Leadership in the global open government movement

The Open Government Partnership (OGP) is the leading global, multilateral organization focused on issues of openness, transparency, accountability and participation. Founded in 2011, the OGP now has 75 member countries and a number of sub-national government members. Canada has been an OGP member since 2012 and has released 3 OGP Action Plans outlining actions it will undertake to make government more open, with a 4th Action Plan currently in progress.

In March 2017, Canada was elected to a 3-year term on the OGP Steering Committee and in October 2018, started serving a 1-year term as lead government co-chair of the OGP. As lead government co-chair for 2018 to 2019, Canada will publish a co-chair strategy outlining the initiatives it will pursue under its key co-chair priorities of inclusion, participation, impact and strengthening the OGP. Canada will track its progress in implementing this co-chair strategy and report quarterly on its work.

In spring 2019, Canada will host an international OGP event, bringing together government and civil society representatives from a number of OGP member countries around the world.

Implementation challenges, risks and mitigation efforts

There will be risks and implementation challenges that will complicate efforts to achieve the digital government vision. Major challenges are outlined below, with reference to how strategic actions outlined in this plan help mitigate these challenges. More comprehensive risk assessments and mitigation plans for each initiative will be included within project plans.

Following are the major challenges to achieving this vision.

Governance

A critical question for digital government will be how organization governance adapts. Traditionally, governments have maintained an emphasis on vertical governance within departments, branches and directorates, with some high-level horizontal governance structures for coordination.

As digital government approaches are implemented, governance and management approaches will need to evolve to fit this new reality. For example, how will greater service integration, data-sharing and tell-us-once approaches change accountabilities?

The governance measures identified in this plan, leadership by the CIO community and the work of governance bodies will help set direction, enable early planning, and develop alignment across government. However, the evolution of governance and management approaches to fit with the digital government approach will be an iterative process that cannot be fully predicted today.

Organizational incentives and culture

Adapting to a new way of doing things will be a big challenge for the public service. For example, promoting a culture of open by default and collaboration by default (working with other government organizations and the public) requires a different way of working and a different way of thinking for public servants; it requires that the public service accepts that it does not have a monopoly on policy advice and knowledge, and that others have valuable information and insights that can contribute to government policy development and service design. Likewise, a public service that uses tell-us-once approaches and integrated services naturally requires a culture that focuses on users rather than organizational silos.

The measures in this strategic plan will begin to address this issue, but all public service leaders need to recognize their role in change management and promoting a digital culture and mindset. Further, changing organizational incentives and culture to align with the digital standards will likely be an iterative process.

Workforce and digital skills

A critical risk to the achieving the digital government vision and implementing the initiatives in this report will be whether the public service has a workforce with the skills and competencies needed, and whether the government can attract, develop and retain top talent.

Initiatives related to recruitment and professional development outlined in Chapter 5 aim to address this and ensure that public service capacity is an enabler of digital government rather than a risk to its implementation.

Morale during digital disruption and transformation initiatives

All change can result in fear and uncertainty, which can be difficult to manage and have impacts on an organization's morale. This is certainly true of digital disruption; however, we must recognize that fear of disruption is not an adequate reason to avoid technological transformation.

Change management will be a major responsibility of departments and leaders going forward. This will involve empathically listening to employees and working to find solutions. Being open by default and working collaboratively can eliminate some fear by avoiding secrecy and speculation.

Professional development initiatives to upskill and retrain workers, if needed, for changing technology or approaches can also assist in addressing the fear of change, as discussed in Chapter 5.

Resources

Resource limitations influence all things, and the government's Digital Operations Strategic Plan will be no different.

A key to staying within resource limits is being strategic about where to focus energy and resources. Prioritization and phasing of initiatives established by departments and governance bodies will assist in adapting to resource limitations, as will phasing out costly legacy systems as appropriate, and adopting better ways of working with the use of APIs, agile procurement and other initiatives identified in this Strategic Plan.

Implementation timing

Delays in projects and transformation initiatives is always a potential risk. The timelines identified in this Strategic Plan are guidelines and, in some cases, aspirational. Updates will be provided in annual rolling follow-up plans with adjustments based on changes in initiative phasing, re-prioritizations and progress reports. Increased use of Agile and procurement simplification discussed in Chapter 4 can also assist in addressing this, as can the wide use of iterative and collaborative processes outlined in the digital standards.

Reporting on the results of the Strategic Plan

Reporting on progress toward digital government will be done through a performance measurement framework for the new Digital Policy, as discussed in Chapter 6. This framework will include digital indicators and show the results of change over time on outputs and, more importantly, outcomes. An accompanying maturity model will be

mapped against the themes in this Strategic Plan and will help assess departmental progress toward implementing the digital government vision, including highlight achievements and leading practices.

Results on the specific strategic action items outlined in this plan will be continually tracked, and progress will be reported as part of future versions of the Digital Operations Strategic Plan to be released on an annual rolling basis.

To supplement this, outcomes and progress will be tracked and reporting on in other mechanisms, as appropriate, such as Departmental Results Reports, performance frameworks, the Government of Canada Service Strategy, the progress report for the Open Government Action Plan and other venues.

Appendix A: detailed list of strategic actions

Filter items [   ]   Showing 1 to 79 of 79 entries

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#1 Section 1.1 **Continuing**, was #48	**Develop digital policy** Changes to IM and IT policies will serve as the foundation of ongoing work to develop a new Digital Policy. The new policy will integrate and evolve Treasury Board policies on service, IT, IM and elements of cybersecurity into a policy that better reflects the current operational environment of departments and drives more transformational change toward a digital government.	TBS	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#2 Section 1.1 **New**	**Promoting user-focused design** To promote the digital standard of "Design with Users," the Treasury Board of Canada Secretariat (TBS) will work with government user experience (UX) practitioners to identify and address administrative barriers to user research, provide guidance on user research practices, and encourage departments to adopt user research methods and activities as a key component of designing and building services, programs and operations.	TBS, with partners	2019-20
#3 Section 1.1 **New**, but based on existing policy requirements	**Service standards and real-time performance reporting** The current Treasury Board Policy on Service has a requirement that priority services have service standards and real-time reporting on the performance of services, and the Government of Canada Service Strategy has identified this as an area of continued focus. In the context of the Digital Policy, consideration is being given to expanding these requirements to cover most or all services. Departments must aim to have meaningful service standards and real-time performance reporting in place for priority services as soon as possible, and should consider establishing different types of service standards to monitor access, accuracy and timeliness for their full range of services.	all departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#4 Section 1.1 **New**, but based on existing policy requirements	**Real-time service application statuses** In the Policy on Service, there is a requirement for departments to develop real-time application status update systems for priority services by November 2017, and the Government of Canada Service Strategy has identified this as an area of continued focus. In the context of the Digital Policy, consideration is being given to expanding these requirements to cover most or all services. Nevertheless, CIOs and departments and agencies should aim make this functionality available to users.	all departments	ongoing
#5 Section 1.2 **New**, evolved from #57	**Develop OneGC vision and Omni Channel Digital Strategy** OneGC is the Omni Channel Digital Strategy for the GC, in which services and technology solutions are designed to be user-centric and interoperable. Omni channel can be defined as a fully synchronized operating model in which the government's service channels present as a single presence to the citizen on any platform, through any device and with any partner. TBS will provide leadership and central coordination for OneGC, including working with partners within and outside the government.	TBS, with partners	TBD

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#6 Section 1.2 **New**, evolved from #51	**Horizontal review on information-sharing** From 2018 to 2020, TBS and key service delivery departments will build on this initial feasibility study and undertake a horizontal review on information-sharing and privacy. This will identify barriers to information-sharing and make recommendations on how to eliminate roadblocks to "tell us once" government services while strengthening privacy oversight. This review will set the foundation for recommendations and potential policy changes in the future.	TBS	2020
#7 Section 2.1 **Continuing**, evolved from #64	**Shift culture and processes toward open by design** To achieve the vision of a more transparent, accountable and responsive government, an "open government" lens needs to increasingly be applied to new or renewed program and service design and at all stages of policy and program development and implementation. The long-term goal is to transform the work processes and culture of the public service to one where programs, services and information are open by design. TBS will lead work that includes designing new processes, protocols and standards to enable and facilitate the proactive release of government data and information by default. The government will continue with Phase 2 of the Open-by-Default project, where we will improve the process of releasing unclassified working documents to the public.	TBS, departments	2021

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#8 Section 2.1 New	**2018 to 2020 Open Government Action Plan** As part of its Open Government Partnership membership, Canada expects to release the 2018 to 2020 National Action Plan on Open Government in fall 2018. The draft plan includes 10 commitments on topics ranging from digital government and services, to open science, to reconciliation and open government. These actions will supplement this Strategic Plan.	TBS, with partners	2018-20
#9 Section 2.1 New	**Access to Information Portal** A new Access to Information and Privacy Online Request Service portal was launched on October 10, 2018. This portal, designed through user testing, uses artificial intelligence to enable requesters to search for summaries of previously released access to information requests and help requesters identify which institutions would likely hold the information they seek. It also allows for electronic payments and electronic transfer of the request to federal institutions. The solution will continue to be iterated through additional user testing, and institutions will continue to be phased in until all institutions (260+) subject to the Access to Information Act and the Privacy Act are receiving requests through this service. To reduce the administrative burden on federal institutions and to improve service to Canadians, efforts are currently underway to digitize the end-to-end access to information and personal information requests by 2021.	TBS	2018

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#10 Section 2.3 **New**, evolved from #74	**Public Service Accessibility Strategy and Action Plan** A Public Service Accessibility Strategy and Action Plan will be released in 2019 to guide efforts to remove barriers to accessing government information and services, and to ensure that all public service employees with disabilities have the tools and support they need to contribute to their full potential. This Strategy and Action Plan will explore what guidelines, training and tools on accessibility by design are needed to ensure that the public service has the expertise and awareness to promote accessible government.	TBS	2019-20
#11 Section 3.1 **Continuing**, evolved from #66	**Incorporate digital principles into operations, programs and service design** In 2018, TBS developed a set of digital standards to guide digital development in the Government of Canada based on international best practices. These principles will guide and shape how government information, technology and service delivery will be managed in a new digital ecosystem. These principles will need to be built into policy, operations and program development, including building accessibility by design, privacy by design, designing with users and working in the open. TBS will be working on socializing these standards across government, and departments should begin to use them to guide their policy, operations and service design work.	TBS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#12 Section 3.1 **New** Strategic Action	**Improving Canada.ca content through targeted user-based initiatives.** The TBS Digital Transformation Office is working on projects with federal departments to make it easier for people to find and understand Government of Canada information and services on Canada.ca. For each project, the office co-creates prototypes, sets concrete usability targets, and runs usability tests with Canadians, trying to improve to address specific questions that people have about specific Government of Canada services. For a prototype to launch, it must make it at least 20% easier for people to get the right answer.	TBS, departments	ongoing
#13 Section 3.2 **Continuing**, evolved from #12	**Better management of mobile applications** As part of the overall web strategy, it was announced in the 2017 to 2021 GC IM-IT Strategic Plan that the government will develop a strategy and framework for the development and management of mobile applications that are easy to use and trusted, with an approval process. Approved Government of Canada mobile applications will be identified on Canada.ca and available through application stores. Before creating a downloadable mobile application, departments should develop clear use cases and determine whether more accessible options will achieve their desired results.	TBS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#14 Section 3.2 **New**	**Compatibility with personal voice assistants** The government is working to make government information easier for personal assistants to search so that these devices could serve as a window to access services in the future. Consistent with the government's policy approach on optimizing for mobile devices, government interfaces through personal voice assistants should be an optional information channel that complements, rather than replaces, other information channels for those that opt in to these third-party platforms.	TBS, departments	ongoing
#15 Section 4.1 **Continuing**, was #3	**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 traditionally have implemented their own ITSM tools. Such 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 departments and tool sets. SSC will put in place enterprise ITSM tools and make them available to all departments. Doing so will bring consistency to the practice of ITSM and, more importantly, reduce the cost and delays of fulfilling service requests.	SSC, departments	2022

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#16 Section 4.1 **New**, evolved from #4, #7, #8, #9, #10	**Workload migration and cloud adoption** Given the risks posed by aging data centres, TBS and Shared Services Canada (SSC) are leading the Workload Migration initiative, working with departments and agencies to migrate their applications from legacy data centres to new infrastructure in either enterprise data centres or cloud services.	TBS, SSC, departments	now until 2023
#17 Section 4.1 **Continuing**, was #5	**Complete telecom/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 (voice over Internet protocol) service. SSC will also work with departments 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	SSC, departments	TBD

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#18 Section 4.1 **Continuing**, was #35	**Ensure IT infrastructure sustainability** A sustainable funding model must take into account the regular renewal cycle of IT infrastructure assets and the appropriate level of investment. TBS and SSC will explore alternative financial and service delivery models to address IT renewal. Budget 2018 announced significant funding over 6 years to improve the management and provision of IT infrastructure for the Government of Canada. A revised funding model will complement these new investments, with a goal of ensuring that a clear and predictable funding source is available for both existing and new IT infrastructure requirements.	TBS, SSC	2023
#19 Section 4.1 **Continuing**, was #50	**Establish SSC asset inventory and baseline** SSC will create an inventory of assets to establish a baseline that can be used to inform prioritization discussions at the Committee on Enterprize Priorities and Planning (CEPP) and ensure that work is focused in the most important areas, such as evergreening and managing organic growth.	SSC	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#20 Section 4.1 **New**	**Network connectivity** The government requires a diverse network landscape to deliver on its digital government vision. To begin, high-performing Internet service is required to enable citizens' interactions with their government through multiple channels, as well as public servants' use of digital, telepresence and cloud-based tools. In this way, reliable and responsive networks will be the highway upon which the government's data travels. In parallel, the government will continue to support special purpose networks, such as the Government of Canada's secret network and science network. Dedicated, reliable network connections to cloud service providers are also a prerequisite to government cloud adoption at an enterprise scale, ensuring CIOs can fulfill their cloud-first policy requirement. This diverse landscape of networks will continue to evolve as data volumes increase and locations of data change over time.	SSC, TBS	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#21 Section 4.2 **Continuing**, was #16	**Secure the government's evolving perimeter** Although the Internet is a game changer in how the public service accesses and shares information, it also brings considerable risk. Malicious software (malware) can compromise any number of these platforms and seriously impact digital systems and disrupt government operations. As the government adopts alternate service delivery models such as public cloud and hybrid clouds, it must continue to provide a secure, reliable and interoperable service delivery environment for internal services and business applications that are hosted in cloud−based environments. At the same time, the government must continue to protect against cyberthreats at critical ingress and egress points on the government enterprise network, both on premises and in the cloud. The government has implemented world-class monitoring services and defensive measures at its network perimeter through SSC-managed gateways. To address risks to its network, the government is standardizing protection and creating a secure, government-wide perimeter that will protect government data both on premises and in the cloud. TBS, the Communications Security Establishment (CSE) and SSC are establishing additional trusted interconnection points between the government network and external partners to: • provide standardized and secure connectivity with external partners and the Internet • act as a gateway to cloud services	TBS, SSC, CSE	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	• protect cloud-based workloads from direct attacks from the Internet Departments that do not currently use SSC Internet services will be migrated to the SSC-managed enterprise network and will use SSC Internet services exclusively. These actions will reduce the risk of rogue, ad hoc or unauthorized connections to and from the government's networks. They will also enhance the government's ability to monitor data that crosses the government perimeter and ensure maximum protection of government information assets. In addition, with government workloads now shifted to the cloud, the government must adapt its approach to securing this evolving perimeter, including applying an information-centric approach. By establishing a risk-based adaptive service that protects the information systems and data processed and stored in cloud-based government digital services, the government will fulfill its cloud-first policy requirement while maintaining continuous awareness of the cyberthreat landscape.		

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#22 Section 4.2 **Continuing**, was #17	**Implement end-point security profiles** Malicious parties frequently seek out exposed or misconfigured public-facing services or equipment to gain access to IT systems and information. End-point devices such as laptop computers, tablets, mobile and portable devices, and servers provide a doorway for such threats. Malware, rootkits (software tools to gain control of a system) 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 expose organizations to unnecessary risk. The goal of this initiative is to evolve end-points to be more resistant to attack and reduce security incidents due to insecure end-points. As successful attacks cannot be realistically eliminated, an associated goal is to limit the damage that can occur when an attack succeeds. In addition to establishing administrative processes and tools to proactively quarantine threats when identified, making the government's end-point devices more resistant to attacks is key to securing the government enterprise. Recognizing the risk posed by misconfigured end-point devices, SSC, in consultation with TBS and CSE, will develop end-point device profiles, for use by departments and agencies. These standardized profiles will be based on	TBS, SSC, CSE, departments	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	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) and user agents to facilitate data-sharing will be implemented to further ensure the integrity of systems and information.		

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#23 Section 4.2 **Continuing**, was #18	**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 intrusion and potential loss. Failing to promptly apply security-related patches and updates can result in exposed vulnerabilities and may lead to serious security incidents. Applying patches to operating systems, applications and devices is a critical activity in ensuring the security of systems, maintaining trust in connected assets, and reducing the government's attack surface. Good configuration management practices includes patch management and will alleviate one of the leading causes of security issues in large enterprises. TBS and SSC will implement an enterprise-wide vulnerability and patch management capability to systematically detect and remediate vulnerabilities. Departments will: • implement these tools and processes • meet standard timelines for remediation • ensure quick response times for emergency or critical patch deployment	TBS, SSC, departments	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#24 Section 4.2 **Continuing**, was #19	**Manage and control administrative privileges** Departments also need to manage internal risks to the security of their IM and IT environments. Privileged accounts (such as those of local or domain administrators and those of other users who have elevated access) are the most powerful accounts in any organization and are therefore appealing targets for attackers. TBS, SSC and departments will work together to minimize the misuse of any account that has elevated privileges, either malicious or accidental. They will implement tools and processes to ensure that all privileged accounts are managed, controlled and monitored properly, and have strong authentication mechanisms (for example, multi-factor authentication). Departments will also implement measures to manage and control the life cycle of and access to privileged accounts, including: • privileged account management processes and technologies • audits and reviews to confirm validity of privileges • continuous monitoring to look for uncharacteristic behaviour	TBS, SSC, departments	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#25 Section 4.2 **Continuing**, was #20	**Protect transactions to and from external-facing digital services** As more Canadians interface electronically with the government, the amount of sensitive information transferred to and from government services will increase. To maintain maximum trust in online transactions, the government must protect them. Implementing secure protocols by default, such as HTTPS, DNSSEC and DMARC, along with approved encryption algorithms, increases the level of confidence that users are accessing a legitimate service and that their communications remain private and free from interference while offering a level of security and privacy that users expect from government services. TBS has established an "HTTPS everywhere" standard that requires departments to use the HTTPS protocol for all external, publicly accessible websites and web services and will continue to monitor departments' progress in implementing the standard. TBS will continue to develop guidance to ensure that web services that serve primarily non-browser clients, such as APIs, are also configured with HTTPS by default.	TBS, SSC, departments	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#26 Section 4.2 **Continuing**, was #21	**Implement a trusted digital identity for public-facing services** A trusted digital identity system is fundamental and a key enabler to seamless and frictionless security, in digital systems. Today, Canadians and the general public can securely access Government of Canada online services by signing in with an online banking credential (such as username and password) from Canadian financial institutions through the Credential Broker Service, or they can use the Government of Canada–branded credential service, known as GCKey. The existing cyber-authentication service is evolving and has been rebranded as Sign-In Canada. Building on the existing solution and maintaining an enterprise approach, TBS and SSC are developing a renewed cyber-authentication service. The goal is to enable the service to accept trusted digital identities from provincial and territorial governments in addition to credentials provided by the private sector. The service is designed to be cost-effective, secure and convenient for users, meet current business needs, and support enhanced functionality required for future federated identity and digital service delivery initiatives. By adopting approved trusted digital identity frameworks, the government will establish a common approach that will facilitate connections with various levels of government across Canada. Using open standards will increase usability and improve interoperability of private sector credentials and internationally accepted trusted digital identities within a larger standards-based digital identity ecosystem.	TBS, SSC	2020

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	In developing public-facing digital services that require authentication, departments will use this common enterprise solution.		
#27 Section 4.2 **Continuing**, was #22	**Implement an internal authentication service for government workers** The intended outcomes for internal identity, credential and access management include: • reduced costs while increasing integrity of business processes for establishing the identity of government workers • promotion of interoperability • improved end-user experience by reducing the need for multiple user IDs and passwords Under TBS's leadership, SSC will implement an internal identity and credential management service tailored to the level of assurance required for particular business processes. For example, a unique digital identity will be needed to authenticate employees, contractors, trusted guests and any other authorized users who access internal government networks and systems. Departments will migrate applications to this enterprise service when their applications are upgraded as part of regular life-cycle maintenance of assets and will ensure that new applications integrate with this enterprise service when implemented.	TBS, SSC, departments	2020

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#28 Section 4.2 **Continuing**, was #23	**Implement an enterprise-secure communications service for classified information** Every day, departments 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 departments to safely share classified information, there is no common solution implemented government-wide. Established by SSC, under the strategic direction of TBS and supported by CSE, the Government of Canada Secret Infrastructure (GCSI) 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. Departments will leverage this service to ensure classified information is managed accordingly. Classified voice and mobile capabilities will also be implemented for users who need to regularly discuss classified information.	TBS, CSE, SSC, departments	2021

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#29 Section 4.2 **Continuing**, evolved from #24	**Improve enterprise data loss prevention** As the government becomes more open by default, it must ensure that sensitive and protected information is not disclosed inadvertently. Preventing the unauthorized transfer or release of sensitive information involves first identifying sensitive data and then protecting it through adequate encryption and access controls. Unauthorized data flows and operations must be monitored, detected and blocked. TBS has established a framework to support an enterprise approach to data loss prevention that relies on an information life cycle and IM solutions. SSC, with departments, will implement the framework to minimize the risk of unauthorized disclosure and inadvertent leakage of that sensitive government data.	TBS, SSC, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#30 Section 4.2 **Continuing**, was #25	**Enable comprehensive understanding of end-point devices** Shifting from a traditional network-centric approach to one that focuses on protecting its information throughout the government and beyond increases the required trust level of the components in the system used to access the information. Understanding user behaviour and the set of assets that underpin a digital environment is essential to knowing what to protect, and enables the government to be more proactive and efficient when responding to threats and attacks. Asset and configuration management are key elements of ensuring system security. The government must be able to proactively and accurately determine and monitor: • the existence and status of all end-point devices • what is running on them • who is accessing them Ensuring that end-point devices (for example, desktop, laptop, tablet and mobile devices) that pose a risk to the enterprise can be identified allows the government to be more effective when responding to threats and attacks. Understanding the landscape requires an understanding of the assets in the government environment. Supporting mechanisms that automate the gathering and analysis of the inventory of assets are critical to ensuring service efficiency amid a growing set of connectable devices, both controlled and not controlled. Under TBS's leadership, SSC and other departments will acquire and implement tools and processes to enable a real-time,	TBS, SSC, departments	2022

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	enterprise view of the current status and configuration of government end-point devices. Such information includes: • hardware and software versions • operating system versions • patch installations		

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#31 Section 4.2 **Continuing**, was #26	**Enhance awareness of the enterprise cyberthreat and risk environment** Departments 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 effectively managing enterprise-wide risk is understanding the changing cyberthreat landscape (for example, who is trying to exploit government networks and systems, by what means, and for what purpose). A better understanding of the threat environments allows organizations to take a risk-based approach and focus cybersecurity efforts and resources rather than attempt to protect against all possible threats. Departments indicate a strong desire for a more proactive approach for government cybersecurity that emphasizes research and innovation in order to keep pace with emerging threats, technologies and trends. Departments have a strong desire to work cooperatively to: • improve the government's security environment • reduce barriers to collaboration and sharing of information TBS is establishing a centralized capability to conduct governance, risk and compliance management activities in order to gain a holistic picture of cyber-related business risks in the government. This capability pulls together data from multiple sources, for example, threat assessments, risk	TBS, CSE, departments	2020

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	registers, investment plans, audit results and critical asset listings, to feed a consolidated enterprise view of cyber-risks. TBS and CSE will work, with support from SSC, and in collaboration with departments, to establish holistic data sharing across all boundaries and levels of IT security within the government, which is essential to ensuring full awareness of activity on the growing and increasing attack surface. Further, continuous monitoring of the cyberthreat and risk landscape will inform decision-making and influence how corrective actions are prioritized across the enterprise to ensure maximum protection of government assets. Automated information-sharing will ensure that the information that security operations teams requires is provided on an ongoing and consistent basis, in a timely manner, from both vertical and horizontal sources, within and from outside the government. Ultimately, comprehensive awareness and understanding of the business technology environment requires establishing a collaborative information-sharing culture.		

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#32 Section 4.2 **Continuing**, was #29	**Document roles and responsibilities for IT and IT security** Departments have a role in managing and delivering IT. TBS will work to elaborate and document the roles and responsibilities of departments, SSC, Public Services and Procurement Canada (PSPC) and central agencies for delivering IT services and implementing the government's digital Strategic Plan so that roles and responsibilities are clearly defined, communicated and executed. They will be clarified through the new Digital Policy. TBS will also continue to provide clear direction to departments on IT security roles and responsibilities, including security-control objectives and other security-related requirements.	TBS	2017

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#33 Section 4.2 **New**	**Improve insider threat protection** Although external threats to the government pose a great risk to the disruption of services and unauthorized disclosure of government information, threats also exist within the government. With its responsibility for maintaining large amounts of sensitive data, the government needs to minimize the risk of unauthorized disclosure. Those with access to internal networks are often identified as a primary target for external attackers. As a means of compromising networks, external attackers are willing to engage in more forceful behaviour such as bribing key support and maintenance staff to attack IT assets from within government networks and information systems. Yet, organizations are much more likely to have an accidental breach as a result of employees' activity than they are to have a malicious one by an outside actor. The vast majority of breaches occur as a result of compromised user credentials through social engineering, which can be largely mitigated through proper training. Balancing the government direction of "open by default" with the security requirements of compartmentalized information, access controls will be designed to take into account role-based access and limit the exposure to information loss. Security screening practices must provide reasonable assurance that individuals can be trusted to safeguard government information, assets and facilities, and to reliably fulfill their duties. TBS will improve how security screening information is shared across departments.	TBS, departments	TBD

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#34 Section 4.2 **New**	**Improve secure application development** Ensuring that software is doing what it is supposed to securely and resiliently is a key aspect in the protection of sensitive information. Software applications are rarely defect-free, and many common defects can be readily exploited by unauthorized parties. Pilots and iterative development should seek to identify potential security issues during development and testing phases because the cost of removing defects and security flaws can be substantially higher after deployment government-wide. Applications that store, process, handle or have network access to sensitive information should be developed with security in mind from the start. Improving software security practices will help the government to reduce vulnerabilities and maximize the usability of applications while maintaining security in the development phase. Iterative development methods (such as agile development) require a well-integrated security discipline to build or update software functionality, analyze software security risk, test for security vulnerabilities and address security-related defects. To support the delivery of a consistent approach to security across the government, TBS will establish an application security framework to enable a developer-centred security approach by integrating security in application development practices. Guidance on best practices to support secure coding practices that considers security testing and reviews, incorporated into each phase of the software development life cycle to help	TBS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	mitigate risks of vulnerabilities in application software, will provide assurance that the government's digital services are operating as intended. Departments will apply the framework when developing and implementing digital services.		
#35 Section 4.2 **New**	**Establish a government vulnerability disclosure framework** The government is underpinned by expansive and complex IT systems that are connecting to the Internet at an increasing rate. Numerous software programs and applications support the government in providing programs and services, and thus it is essential to ensure that the software used by the government can be trusted. However, vulnerabilities and bugs are constantly being discovered in software programs that, if exploited, could put government networks and information at risk of compromise. At times, vulnerabilities may also be identified by parties outside the government. TBS, in collaboration with CSE, will establish a framework that will provide the roadmap for the development of a strong responsible disclosure program to help the government find out about and address risks quickly in order to assist in the protection of digital services. Departments will adopt the framework and ensure alignment with existing departmental cyber and IT security event management plans.	TBS, CSE	2020

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#36 Section 4.2 **New**	**Evolve cyber-event management plans** Cybersecurity events related to government information systems can have a significant impact on the delivery of government programs and services to Canadians and, consequently, confidence in government. The ability to respond to cybersecurity events in a consistent, coordinated and timely manner across the government is essential to ensure the security and resilience of government program and service delivery. Effective incident management is key to limiting the disruption caused by an incident and restoring normal business operations as quickly as possible. TBS will update the Government of Canada Cyber Security Event Management Plan (GC CSEMP) to ensure that the operational framework for the management of cybersecurity events (including cyberthreats, vulnerabilities or incidents) is continuously improved. The plan will be tested and reviewed annually, and modified as required. This includes annual tabletop exercises to ensure that cybersecurity events are addressed in a consistent, coordinated and timely fashion government-wide. Departments will update existing cybersecurity event management or incident response plans to align to the GC CSEMP.	TBS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#37 Section 4.3 **Continuing**, evolved from #32	**Adopt agile approaches to implementing business solutions** It is a challenge to be able to acquire goods and services in a timely manner to operationalize government mandates that provide value to citizens. TBS and PSPC are leading a government-wide initiative to identify and support key improvements in the federal procurement regime. Departments 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 business requirements, departments will contact TBS to discuss other options. Departments are required to keep TBS up to date on their investments and plans. Where a customized or in-house solution is the only option, application development teams should take modern and agile approaches to achieve greater speed and agility. They must also take into account the increasingly complex ecosystem of interdependent software architecture, infrastructure and processes. Departments will promote a learning culture that allows 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 • engage functional (IM) experts early in the development process	TBS, PSPC, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	• adopt an approach that considers a service-oriented architecture and application programming interface (API) first rather than large and complex constructs		
#38 Section 4.4 **Continuing**, evolved from #6	**Government email solutions** Departments have traditionally operated their own email systems, resulting in business and cost inefficiencies. SSC as the service provider and TBS as the enterprise business owner are developing a strategy for next-generation email services for the opportunity to procure a larger suite of communications tools for the government, including email services. To align with this direction, the current suite of GCTools will evolve into an Open and Accessible Digital Workspace. To ensure stability, service continuity and facilitate transition to a new solution, SSC will upgrade legacy email environments.	SSC, departments	TBD

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#39 Section 4.4 **Continuing**, evolved from #11	**Build a platform for enterprise interoperability** The government knows that a platform for enterprise interoperability will lay the foundation for achieving the government vision for data-sharing of getting the right information to the right people at the right time. TBS will continue to work with stakeholders to provide a digital exchange toolkit: a suite of modern integration tools to serve the needs of a digital exchange ecosystem. Examples of components in this toolkit are the GC Service Bus, the Digital Exchange Platform and the API Store. These components enable the secure exchange of data between enterprise systems, departments, governments and the public. The toolkit provides scalable, reliable and industry-leading technology solutions for departments to leverage to more rapidly implement data exchange use cases. The capability to link internal departmental information with solutions for delivering programs and services will enable greater government-wide collaboration when designing digital services. This approach will also enable business process improvement within the government and across jurisdictions, leading to improved program and service delivery for citizens and businesses. Through the creation and use of a governance framework (policies, directives, guidelines and open standards) for the digital exchange ecosystem, TBS will: • foster openness and collaboration • promote digital services	TBS, PSPC, SSC	2019

Action items ↑↓	Comments or descriptions ↑↓	Accountability ↑↓	Timeline ↑↓
	• advance enterprise interoperability and information-sharing across the government		
#40 Section 4.4 **Continuing**, was #52	**Introduce a strategy for use of open source software and open standards** The use of open source software supports interoperability and information-sharing and should be considered in the assessment of IM-IT solutions. Open source products are publicly available, and the availability of their source code promotes open and collaborative development around their specifications, making them more robust and interoperable. The use of open standards ensures interoperability between products and systems, and maintains flexibility within the IM-IT environment. TBS will continue to run the Open Source Advisory Board and working group, as well as lead development of a strategy, including open source licences framework guidance, an open-first white paper and an open resource exchange, to set direction for the government on the use and release of open source software and open standards that will be ratified by the Government of Canada Enterprise Architecture Review Board (GC EARB).	TBS	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#41 Section 4.4 **Continuing**, was #53	**Develop an application programming interface strategy** APIs are used to reveal government digital capabilities and can be combined and reused to create digital services. APIs are increasingly becoming the way to facilitate sharing of government data and information and, as such, are foundational building blocks that support the government's commitment to digital services. TBS will develop an API strategy for the government.	TBS	2018
#42 Section 4.5 **Continuing**, was #15	**Advance analytics** 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 analyze them. Big data can make available almost limitless amounts of information, improving data-driven decision-making and expanding open data initiatives. TBS, working with departments, will lead the development of requirements for an enterprise analytics platform. TBS will work with departments to identify a business lead to develop a data lake (a repository of raw data) service strategy so that the government can take advantage of big data and market innovation to foster better analytics and promote horizontal data-sharing.	TBS, SSC, departments	TBD

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#43 Section 4.5 **Continuing**, was #54	**Enhance online infrastructure to enable departments to release their data and information** The government has also worked to support the "demand side" of open data and information, identifying and collaborating with stakeholders in organizations and companies that leverage open government data and information. Canada's Open Data Exchange (ODX) is one organization that helps Canadian companies make use of open data. TBS has worked with the ODX to deepen insight into the commercial open data landscape and to understand what challenges need to be overcome in order to make Canadian open data companies more competitive. In the last 2 years, ODX has incubated 15 new data-driven companies, and has more work planned in future years to continue to promote the use of open government data among Canadian companies.	TBS	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#44 Section 4.5 **Continuing**, was #55	**Develop a master data management program** In an open and distributed operational environment such as the government, there is a risk that business-critical data becomes redundant, inconsistent and scattered throughout the enterprise. Master data management (MDM) can be defined as the processes, governance, tools, rules and technology required to create and maintain consistent and accurate master data. It focuses on common critical data elements and establishes strong governance around them. MDM can eliminate redundancy and inconsistency of data in an organization and ensure its quality and control. It can provide a single, authoritative point of reference that can be shared by many processes and applications across the organization. It can also streamline data sharing and facilitate interoperability. TBS will work with Statistics Canada and other key business owners to establish a government-wide MDM program to formally identify standard data elements and single authoritative sources for key information domains, where appropriate.	TBS, Statistics Canada, departments	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#45 Section 4.5 **Continuing**, was #56	**Implement GCDOCS** Time and productivity are frequently lost due to the lack of consistent tools and systems to help employees store, search and find the information and data they need to do their jobs. Enterprise IM solutions such as GCDOCS streamline and simplify these processes, but they need to be configured properly to make back-end IM processes as invisible as possible to users. Automation can provide opportunities to: • simplify and streamline key IM processes and practices • deliver a seamless user experience that relieves burden on individual government workers Furthermore, implementing integrated and standardized solutions across departments can help make it easier for government employees to find, use and share the information and data they need to do their jobs, while ensuring consistent, foundational management of government information assets. Information and data can be leveraged to help departments achieve their business objectives and meet their mandated requirements. TBS and PSPC will enhance the government-wide GCDOCS service for departments, including: • full deployment by 2022; 30 organizations have fully adopted GCDOCS, an additional 79 organizations are in various stages of onboarding • broadening its integration with back office systems	TBS, PSPC, departments	2022

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	• piloting its use as a tool for increasing the openness of government information		
#46 Section 4.5 **Continuing**, was #60	**Standardize metadata** Metadata is the backbone of digital automated processes, information retrieval, and the use and sharing of information and data. Metadata defines and describes the structure and meaning of information and data and of the context and systems in which they exist. Metadata supports efficient and effective management of information and data resources over time, which facilitates decision-making, accountability and the efficient delivery of government programs and services. Standardized metadata supports: • interoperability within and across systems • reuse of information resources within, across and outside the government Along with standardized metadata, consistent use of authoritative vocabularies supports the exchange of information and data resources within and across systems. Automated metadata collection, creation, use and reuse can greatly relieve burden on individual government workers. TBS, in conjunction with business owners, will standardize metadata schemas and maximize their benefits to simplify and automate metadata usage and make it invisible to users.	TBS, departments	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#47 Section 4.5 **Continuing**, was #63	**Provide tools and resources to make innovative use of information and data** The need for tools to collect, store, analyze, manage, share and visualize data is increasing in all departments. Enabling open standards, open source, interoperability, and the sharing of expertise requires access to a common set of data tools commensurate with common data needs. At the same time, departments need a flexible framework to explore new tools and more advanced options that are both interoperable and secure. The Government of Canada's IT infrastructure must be able to support the ambitious agenda of its data system. There is a growing need for higher computing capacity and for the modernization of older data infrastructures. For example, collaborative efforts are underway through initiatives such as the Canadian Geospatial Data Infrastructure. This initiative provides national geospatial standards and infrastructure critical to address environmental assessments, emergency response and space program continuity. It is important that the government take a proactive approach in addressing its future data requirements. Currently, many departments and agencies are anxious for the delivery of secure cloud infrastructure and/or procurement options. It is expected that public Protected B cloud services will be ready for departmental access by spring 2019. • TBS will work with departments and agencies to identify common business requirements, develop a catalogue of recommended and pre-approved tools, and establish	TBS, SCC, departments	2020

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	updated guidelines and processes for their implementation. • TBS and SSC will assess required infrastructure needs over the short and medium terms (that is, trajectories based on historical data usage, data pressures on the network and bandwidth consumption, and forward-looking opportunities) and provide an interim report to DM CEPP by end of summer 2019. • TBS and SSC will provide a final report to DM CEPP by fall 2020, factoring in all organizational data strategies.		

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#48 Section 4.5 **New**	**Develop a data strategy for the Government of Canada** Under direction from the Clerk of the Privy Council, TBS has been co-leading the development of a Data Strategy Roadmap with the Privy Council Office and Statistics Canada since January 2018, working with other departmental partners. The roadmap identifies strategic priorities for a unified and collaborative approach to manage government-wide data as an asset while respecting privacy. Implementation of the Data Strategy Roadmap aims to support improved decision-making and enhanced services to Canadians and a more transparent, collaborative and digitally enabled public service. Recommendations in the roadmap are oriented around 4 themes: 1. stronger leadership and governance 2. improved data literacy and skills 3. enabling infrastructure and legislation 4. treatment of data as a strategic asset The goal is to set a foundation so that the government creates more value for Canadians from the data we hold while ensuring the privacy and protection of personal information. Given the importance of data to supporting a digital government vision, the initiatives in the Data Strategy Roadmap complement, may overlap with, and are in some cases identical to the priorities identified in this Strategic Plan.	TBS, Privy Council Office, Statistics Canada	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#49 Section 4.6 **New**	**Artificial intelligence** The use of automation and artificial intelligence also requires careful attention to the issues of potential bias, impacts on diverse populations, risk, and managing compatibility with administrative law. To begin to identify and navigate these issues, TBS developed a working paper on the responsible use of artificial intelligence in the Government of Canada using an open-by-default and collaborative approach that engaged experts, industry professionals and the public. Work is now ongoing in developing a Directive on Automated Decision-Making and an Algorithmic Impact Assessment to provide an assessment framework that helps institutions better understand and mitigate the risks associated with automated decision-making systems by providing the appropriate governance, oversight and reporting, and audit requirements. The tool is being developed with open collaboration. As more use cases of automation and artificial intelligence are explored and adoption advances, more policy guidance, tools and training will be developed to help ensure that departments and public servants are using this technology in innovative and responsible ways.	TBS, departments	2019
#50 Section 4.6 **New**	**Blockchain pilots** Blockchain use cases and the practicality of blockchain-based applications are still being explored by governments around the world. The government announced in July 2017 the intention to run at least 6 select pilot projects on the use of blockchain.	TBS, departments	TBD

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#51 Section 5.1 **Continuing**, was #41	**Modernize workplace technology devices** Workplace technology devices are essential for a modern workplace and a collaborative, mobile workforce, as outlined in the Blueprint 2020 vision. TBS will work closely with departments 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 secure configurations. SSC will continue to consolidate contracts and procurement activities to improve security, reduce costs and improve service to Canadians. SSC will also procure workplace technology devices and work with TBS and other departments to standardize devices. Departments are responsible for supporting and maintaining 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.	TBS, SSC, departments	ongoing
#52 Section 5.1 **Continuing**, was #42	**Support a mobile workforce** The government is committed to and encourages an open and collaborative work environment where mobile devices are used. TBS will develop a mobility strategy, focusing initially on smartphones. Departments will balance the cost of these devices, and their support, against the business value achieved.	TBS, SSC, departments	2020

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#53 Section 5.1 **Continuing**, was #43	**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 will implement Wi-Fi access to networks for all employees within common areas and their workspaces, where the job requires mobility. Departments 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.	TBS, SSC, departments	2020
#54 Section 5.1 **Continuing**, was #44	**Provide desktop video-conferencing to employees** Increased access to video-conferencing supports the collaborative operations of virtual teams across departments, time zones and regions. Departments will complete the re-engineering of their in-house video-conferencing facilities to enable full interconnectivity across the government. Where appropriate and where a user profile supports such functionality, SSC will also create the network and bandwidth capacity needed to support video-conferencing at desktops.	SSC, departments	2021

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#55 Section 5.1 **Continuing**, was #47	**Advance digital collaboration** GCTools such as GCpedia, GCconnex, GCcollab, instant messaging and the GCintranet increase productivity and enable collaboration across the government and other partners. Employees are able to easily connect and share information and work across departments and geographic boundaries, resulting in better service to Canadians. GCTools that support government requirements for accessibility, official languages and collaboration with external partners will be further developed and integrated into other applications. The current suite of GCTools will evolve into an open and accessible digital workspace, which will allow employees to easily connect with the information, colleagues and external partners they need to work effectively. The open and accessible digital workspace will also provide 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 and regions that provide support to teams using GCpedia, GCconnex and GCcollab to enhance their work. Departments will decommission stand-alone collaborative platforms unless they are linked to core local business requirements. Email communication will be	TBS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	reduced in favour of open discussions or instant messaging, where transitory communications can occur without bogging down government systems.		
#56 Section 5.2 **Continuing**, was #39	**Enable career development** Further enabling IM-IT professionals to evolve into new roles and functions, and addressing competency gaps in areas such as strategic thinking, influencing, innovation, collaboration and agility, requires investment in employees. To support IM-IT professionals, retain talent, and re-skill or upskill the workforce, emphasis will be placed on: • a career management portal • learning provider solutions TBS, in conjunction with the Canada School of Public Service (CSPS), will lead work in this area.	TBS, departments, CSPS	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#57 Section 5.2 **Continuing**, was #46	**Promote digital literacy and collaboration** Digital literacy goes beyond basic computer skills. It is essential to make the most of investments already made in the IM-IT environment, devices and tools, and to ensure that IM-IT helps workforce productivity rather than detracts from it. Data literacy is a skill required for working digitally. Government employees need to be able to extract high-value insights from the wealth of available information and data and to communicate them. TBS will develop partnerships to leverage and design an engagement and awareness program for all public servants to enable them to: • become more data-literate • leverage evidence-based decision-making • engage internally and externally as digital citizens Public service employees should also be able to use GCTools such as GCpedia, GCconnex and GCintranet to share information and 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 will nurture these skills throughout the public service by: • adopting and using GCTools for everyday work	TBS, CSPS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	• 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 departments and to demonstrating the full benefits of these collaborative tools. Leaders will adopt an "open first" approach toward content creation and encourage their employees to participate in shared knowledge and collaborative digital spaces, other than where security requirements prohibit such an approach.		

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#58 Section 5.2 **Continuing**, was #70	**Modernize the information and data management profession** Revitalizing the information and data management profession is necessary to ensure that it keeps pace with current and emerging business needs in a digital, open and service-oriented environment. Furthermore, information and data professionals should be more involved early on in the development process when designing or renewing programs and systems to ensure that issues associated with information and data management and sharing are proactively considered. Realigning roles and responsibilities of information and data management professionals and other key stakeholders could help improve collaboration and overall coherence. TBS will lead the development of new standardized: • generic work streams and job descriptions • generic competency profiles • organizational structures	TBS	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#59 Section 5.2 **Continuing**, was #72	**Strengthen leadership development** There is a requirement to invest in current and aspiring leaders across the enterprise to: • address talent retention issues • increase capacity to develop leadership competencies Emphasis will be placed on: • talent management and succession planning • learning provider solutions Specific leadership development efforts include: • talent reviews • promoting leadership development programs at CSPS • tracking and facilitating the movement of IM-IT leadership across the enterprise TBS will lead work in these areas.	TBS	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#60 Section 5.2 **Continuing**, was #75	**Expand open government training and outreach** Training and awareness sessions are being provided to public servants across the federal government to enhance knowledge and skills for open government. TBS will continue its work to expand open government training and outreach in the coming years, in partnership with CSPS. In addition to hosting public webinars on open government issues, and developing dedicated open government training and learning activities for public servants, the Government of Canada will develop and publish open government learning materials for use by teachers and post-secondary instructors. This will help Canadians know about our open government work and more actively participate in it, which in turn increases Canada's ability to harness the social and economic potential of open government.	TBS, CSPS	2018

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#61 Section 5.2 **New**	**Enhance digital security awareness and reliability of government employees** The government is shifting its culture to digital and needs a better understanding of basic cyber/security hygiene with respect to digital systems, using services, sharing information and passwords. Improving behaviour and tendencies users have when interacting with systems will allow for a transition in security focus from building guardrails to innovation and evolution in security thinking and implementation. There is a need to ensure that patterns of behaviour are engrained into the daily activities of government staff to ensure a safe and secure digital infrastructure. Canadian Centre for Cyber Security will promote a general approach to training and awareness for IT security and supporting IT security teams across the government.	CCCS, TBS, departments	ongoing
#62 Section 5.2 **New**	**Broaden security innovation, collaboration and creativity in problem-solving** There is a growing need to increase the capability/capacity of teams across the government to work together and develop creative solutions to problems that are being faced across the board. The government will provide a forum or platform to develop solutions and encourage teams to be curious in their own environments and be creative in how they look at managing their assets. Teams will be encouraged to consider pragmatic security solutions as much as innovative approaches; simple solutions that have the ability to enable business success are often an accidental development.	TBS, CCCS, CSPS, SSC, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#63 Section 5.2 **New**	**Assessing public service skills and analyzing future needs** Technological disruption, changing approaches and digital government will require public servants to have new skills and competencies. To help public servants and the public service adapt to this evolving digital environment, TBS will work with partners such as CSPS to identify competencies for the digital age to better understand how the current skills profile of the government needs to evolve.	TBS, CSPS, with partners	2019-20
#64 Section 5.2 **New**, evolved from 71	**A Digital Academy** The Government of Canada is launching a Digital Academy with the goal of increasing the offerings available to public servants who want to increase their digital literacy and understanding of key areas such as service design, data analytics and new technologies as they apply to their work. Informed by examples in other jurisdictions, we will build a made-in-Canada model that will lead to better understanding of how digital can improve how government functions and allow better services. CSPS will lead the delivery of the Digital Academy, in partnership with TBS, the Canadian Digital Service, Statistics Canada, other government departments and partners in the non-profit, academic or private sectors. The development of the Digital Academy will be especially guided by the principles of open by default, collaborating wisely and iterative development. Initial courses were piloted in September 2018, and the government will aim for this service to be available beginning in 2019.	CSPS, TBS, with partners	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#65 Section 5.3 **Continuing**, was #40	**Improve diversity** An inclusive workplace is one where the workforce reflects the full breadth of the talent pool. Diverse teams bring broader perspectives and ideas for greater capacity to find creative solutions and innovate. Currently, IT remains a predominantly male domain. Building on current efforts, initiatives include improving representation via recruitment for women in the CS (Computer Systems) Group. To further support the government's commitments to achieving greater representation and a balanced and diverse workforce, departments will develop and leverage partnerships with organizations that encourage IT as a career choice for young women. Departments and central agencies will also work to increase labour mobility among women by encouraging leaders in the public service and the private sector to consider roles in the government's IT community.	TBS, departments	2017

Action items ↑↓	Comments or descriptions ↑↓	Accountability ↑↓	Timeline ↑↓
#66 Section 5.3 **Continuing**, evolved from #69	**Strengthen recruitment** To address challenges that include branding issues, shortfalls in capacity and competency gaps, the government will focus on a CS recruitment campaigns, enterprise approaches and partnerships to support recruitment efforts and onboarding. Specific initiatives will focus on: • outreach to educational institutions • onboarding tools and initiatives to improve the integration of new recruits • partnership with the Public Service Commission of Canada to create a partially assessed CS inventory TBS, working with departments, will lead work in these areas. Such initiatives will better position the government to address capacity and competency gaps more efficiently.	Public Service Commission of Canada, TBS	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#67 Section 5.3 **New**	**Manage and maintain cyber talent** The government is working toward a future where services for Canadians are user-centric, seamless and digitally enabled. Cybersecurity will remain a key element for protecting the information and maintaining the trust of Canadians when using government services. A robust, skilled and diverse workforce within the government is fundamental in supporting this transformation. However, there is a global shortage of qualified professionals in the cybersecurity domain, which is complex and requires a broad depth of skill sets. This growing gap between the supply and demand for skilled cybersecurity professionals has an impact on the government because it has to compete with the private sector and globally to recruit talent. To compete with the private sector, the government has to address the image that the government is bureaucratic, lagging in technology, slow with recruitment and has limited career development opportunities. TBS must play a lead role in cultivating the federal public service as a model workplace where professional, skilled workers are trained and motivated to serve Canadians. This includes ensuring that there is a constant pool of proficient and capable people to support the delivery of government services for Canadians. There is a need to develop an agile human resource approach to address the skills gap in the Computer Science (CS) and related communities, specifically for the cybersecurity field, to enable a government digital transformation and further strengthen the government cyber posture. TBS will develop a strategy to recruit, retain and	TBS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	train the next generation of cybersecurity talent within the government in order to bolster the government's capacity to deliver the services Canadians expect in a safe and secure manner.		
#68 Section 5.3 **New**, evolved from #73	**Talent Cloud** Talent Cloud aims to creating a thriving marketplace where today's talent can find exciting, high-quality job opportunities in government that fit their passions and talents. This grassroots pilot project includes an experimental new staffing platform for project-based employment, utilizing some of the practices and advantages of the gig economy but avoiding its precariousness. The platform will launch as a working pilot in fall 2018.	TBS with partners	ongoing
#69 Section 6.1 **Continuing**, was #33	**Lead innovation** The role of departmental CIOs is evolving from IM-IT service providers into strategic business partners, innovation agents, business enablers and catalysts for enterprise transformation. CIOs are innovation agents, business enablers and catalysts for enterprise transformation. Departmental CIOs will be strategic business partners who bring IM-IT to the table in innovative ways to address the department's business needs. To explore working in ways that are more agile, new opportunities with various innovations hubs will be pursued.	departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#70 Section 6.2 **Continuing**, was #30	**Evolve IM-IT management practices, processes and tools** CIOs should plan and execute departmental IT plans so that they align with the government's Strategic Plan for IM-IT and overall enterprise modernization priorities. Important tools to support CIOs include: • investment plans • architectural reviews • application portfolio management • expenditure reporting • performance reporting Optimizing IM-IT investments to meet business outcomes will propel the evolution of IM-IT management processes and tools. TBS policy and guidance will allow departments to: • manage IM-IT consistently and with greater maturity • better understand IM-IT at the enterprise level • evolve digital service delivery • benchmark themselves against similar departments • monitor and track progress against government priorities • set future priorities TBS will also provide policy guidance and more robust project oversight to help departments: • develop sound project cost estimates • implement good project management practices for complex IM-IT projects • guide investments from concept to benefits realization	TBS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#71 Section 6.2 **Continuing**, was #31	**Develop enterprise architectures for business, information, applications, technology and security** Enterprise architecture will be used to provide all government departments with a structured approach to identify and describe government business needs and the information, applications and technology that are required to enable them. Enterprise architectures show: • the capabilities and services being provided to Canadians • the information that supports each government service • the people impacted by business decisions • the secure enabling applications and technologies for each government service Understanding enterprise architecture enables effective decision-making about IM-IT investments, costs and risks, allowing the government to act as one to optimize performance and deliver on government priorities in the digital era. TBS will improve architecture processes and tools established in 2017 and strengthen integration with various processes such as departmental IT planning, application portfolio management and project management and oversight. GC EARB, with representation of business and technology stakeholders from across the government, will continue to work collaboratively to simplify the government IM-IT environment by: • assessing alignment of initiatives • identifying opportunities for reusing solutions that support similar needs	TBS, functional communities	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
	• developing new digital capabilities and innovation opportunities • setting and documenting standards for government technology • providing direction on IM-IT investment		
#72 Section 6.2 **Continuing**, evolved from #34	**Adopt modern and flexible business models** To achieve a better balance between demand and capacity, SSC and PSPC will adopt cost-recovery business models for some IT services. Doing so will provide greater flexibility to provide agile and effective services to the government. As an enterprise, departments will achieve better business value by sharing IT resources, capacity and capabilities. Based on the draft principles and framework developed in the 2017 to 2018 fiscal year, SSC will continue to work with its partners to finalize the model, including making adjustments to reflect the impact of funding decisions from the 2018 federal budget and the continuing evolution of the IT delivery environment. The goal remains to implement a new funding model beginning in the 2019 to 2020 fiscal year.	SSC, PSPC	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#73 Section 6.2 **Continuing**, was #36	**Rationalize investments** In keeping with enterprise IM-IT governance, spending on new or significant changes to certain IM-IT and IT-enabled projects will be subject to consultation with TBS. Consultation will include discussions on spending for systems for common business domains such as: • case management • IM • human resources management • financial management • other back office administrative processes • identity and credential solutions • IT infrastructure and associated solutions Departments will take an enterprise approach to managing their portfolio of applications to: • determine opportunities for common, government-wide solutions • retire aging and at-risk applications Applications that remain in use and that support mission-critical business functions are to be kept evergreen until they can be replaced by modern solutions.	TBS, SSC, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#74 Section 6.2 **Continuing**, was #58	**Introduce stronger project oversight at the concept phase** TBS will enhance and strengthen the oversight function for IT-enabled projects by introducing earlier reviews of investment concept cases. Such reviews will take place prior to defining the solution or the project to implement the solution, allowing for early engagement and setting of direction. For high-risk project investments, TBS will monitor and report on performance and governance throughout the life of the project. Better management of project investments, coupled with an agile approach to development and delivery, maximizes value and reduces service delivery costs, enabling the government to respond more rapidly to emerging issues.	TBS, departments	2019
#75 Section 6.2 **New**, evolved from #62	**Developing a Digital Performance Measurement Framework and Maturity Model** To measure progress on digital transformation, a performance measurement framework will be developed to accompany the Digital Policy. A maturity model will accompany this framework to assess departments on digital government adoption, mapped to the themes included in this Strategic Plan. Data and insights generated from this process will support a continuous improvement process to inform evolving digital priorities or identify potential barriers to progress toward digital government that should be addressed.	TBS	2019

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#76 Section 6.2 **New**	**Reviewing and updating governance committees** To ensure that our whole-of-government governance approach is appropriate to the needs of a digital government, TBS will be reviewing and updating enterprise governance, including committee mandates and memberships.	TBS	2019-20

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#77 Section 6.3 **Continuing**, was #67	**Advance financial management transformation** Financial Management Transformation (FMT) is modernizing the financial and materiel management (FM) business model across the Government of Canada, to provide more timely access to reliable, consistent GC-wide information, and ensure that FM services better enable the delivery of programs for Canadians and remain cost effective and sustainable. FMT does so by designing standard, streamlined processes and common data structures, building modernized common systems to replace departmental platforms, helping managers, employees and financial and materiel management specialists to adopt new processes and systems, and aligning financial management systems investments with government priorities. FMT's near-term focus is to implement the digital core of the Government of Canada Financial and Materiel (GCFM) solution. The GCFM digital core will deliver SAP S/4 functionality common to each department to manage finance, materiel, and other administrative activities in real-time. This common platform will deliver a standardized and streamlined approach across Government of Canada departments and agencies to drive an effective digital government.	TBS, departments	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#78 Section 6.3 **New**	**Leadership in the global digital government movement** In 2018, Canada signed the Digital 7 (D7) charter, joining leading digital nations in a mission to harness digital technology to the benefit of citizens. The D7 charter commits Canada to working toward core principles of digital development, with a focus on user needs, open government, and a commitment to share and learn from D7 member nations. D7 comprises nations that are recognized as having the most advanced digital governments globally. It provides a forum for member nations to share best practices, identify how to improve service delivery to citizens, collaborate on common projects, and support and champion their respective growing digital economies.	TBS	ongoing

Action items ⬆⬇	Comments or descriptions ⬆⬇	Accountability ⬆⬇	Timeline ⬆⬇
#79 Section 6.3 **New**	**Leadership in the global open government movement** The Open Government Partnership (OGP) is the leading global, multilateral organization focused on issues of openness, transparency, accountability and participation. Founded in 2011, the OGP now has 75 member countries and a number of sub-national government members. Canada has been an OGP member since 2012 and has released 3 OGP Action Plans outlining actions it will undertake to make government more open, with a 4th Action Plan currently in progress. In March 2017, Canada was elected to a 3-year term on the OGP Steering Committee and in October 2018 started serving a 1-year term as lead government co-chair of the OGP. As lead government co-chair for 2018 to 2019, Canada will publish a co-chair strategy outlining the initiatives it will pursue under its key co-chair priorities of inclusion, participation, impact and strengthening the OGP. Canada will track its progress in implementing this co-chair strategy and report quarterly on its work. In spring 2019, Canada will host an international OGP event, bringing together government and civil society representatives from a number of OGP member countries around the world.	TBS	2019

Appendix B: top modernization priorities by theme

This Strategic Plan is expansive, with many strategic actions and concurrent initiatives identified. Sometimes scarce resources or limited time requires prioritization of initiatives.

The following table should be used as a guide for prioritizing competing initiatives. Governance committees will use this list as a starting step when identifying priorities for Shared Services Canada and other internal service providers.

Proposed priorities for the Digital Operations Strategic Plan for 2018 to 2022

Category	Priorities
Service orientation and user-centred	• Developing toward a tell-us-once approach, review of policy barriers to information-sharing (OneGC) [*] • Improving service delivery and compliance with the Policy on Service and the new Digital Policy (all departments) (OneGC) • Expanding user research in service, policy and operations design
Open, collaborative and accessible	• Implementing the Open Government Action Plan [*] • Digital collaboration tools [*] • Creation of a Public Service Accessibility Strategy and Action Plan
Digitally enabled delivery	• Digital Identity Initiative (OneGC) • Any-device compatibility, pilots with digital voice assistants (OneGC)

---

[*] Denote priorities that are continuing from the 2017 to 2021 GC IM-IT Strategic Plan.

Category	Priorities
Modern tech and information stewardship	- IT service management [*] - Stabilize legacy [*] - Departmental Application Strategy, data centre consolidation, and cloud adoption [*] - Government of Canada interoperability (OneGC) [*] - Migration to Government of Canada identity, credential and access management service [*] - Cybersecurity [*] - Network consolidation [*] - Shared case management [*] - Procurement modernization [*] - Data strategy - Artificial intelligence initiatives
Digitally enabled public service	- Workplace technology transformation [*] - Skills development and implementing a Digital Academy - Recruitment modernization and Talent Cloud
Good governance	- Early alignment and review discussions starting at the concept phase, and Government of Canada Enterprise Architecture Review Board [*] - Enhancing project oversight [*]

[*] Denote priorities that are continuing from the 2017 to 2021 GC IM-IT Strategic Plan.

Date modified:

2018-12-27