



Treasury Board of Canada  
Secrétariat

Secrétariat du Conseil du Trésor  
du Canada

Canada

# Government of Canada Strategic Plan for IM-IT 2017-2021 and Updated Cloud Adoption Strategy

Presentation to PSCIOC

October 5<sup>th</sup>, 2017

Charlottetown, Prince Edward Island

Denise Gomes

Senior Director, IT Priorities & Planning



CANADA 150  
1867-2017

# Background

---

- First GC IT Strategic Plan was published in June 2016
  - Provided enterprise-wide IT direction
  - Created linkages between GC priorities, strategies and Departmental IT Plans
  - Committed to an annual update and a progress report to the Secretary in fall 2017

# Purpose

---

- An updated version of the GC Strategic Plan for IM-IT 2017-2021 will be published in October
  - An interim step to a larger Digital Policy and Strategy that are currently under development for 2018-19
  - Outlines strategic actions to strengthen the IM-IT foundation and position the GC to shift its mindset to digital
  - Fulfills direction in Treasury Board Decision Letter to SSC from May 2017
    - “That TBS brings forward a Government of Canada IT Strategic Plan every October that outline government priorities and serves as the basis for SSC’s planning, including its annual Investment Plan.”
- Sets IM-IT direction for the GC and identifies enterprise-wide priorities and key activities for departments, agencies and service provider organizations
  - A key input to the Departmental IT Planning process as an element of the prioritization framework used to identify overall IM-IT investment and work priorities for the GC
- Departments and agencies should use this document to internally prioritize IM-IT investments and initiatives and demonstrate alignment to enterprise direction
- For service provider organizations, it identifies foundational priorities and activities that are required to modernize service delivery and improve sustainability

# Changes / Additions since June 2016

- Insight into the digital direction being established by the GC
- Addresses feedback provided through consultation with:
  - The public in summer and fall 2016
  - The GC Chief Information Officer (CIO) and Information Management Senior Official (IMSO) communities in February 2017
- Key changes:
  - Closes gaps identified through public consultation in the areas of accessibility, open source and procurement
  - Strengthens problem statements and further develops the case for change
  - Addresses the key message from the GC IM-IT community that IT supports IM, which must support the business
  - Integrates Treasury Board Decision Letter directions

This version brings together the foundational enablers of information, data, technology and security required to deliver open and transparent government and improved services to Canadians.

# Vision and Drivers

---

## Vision

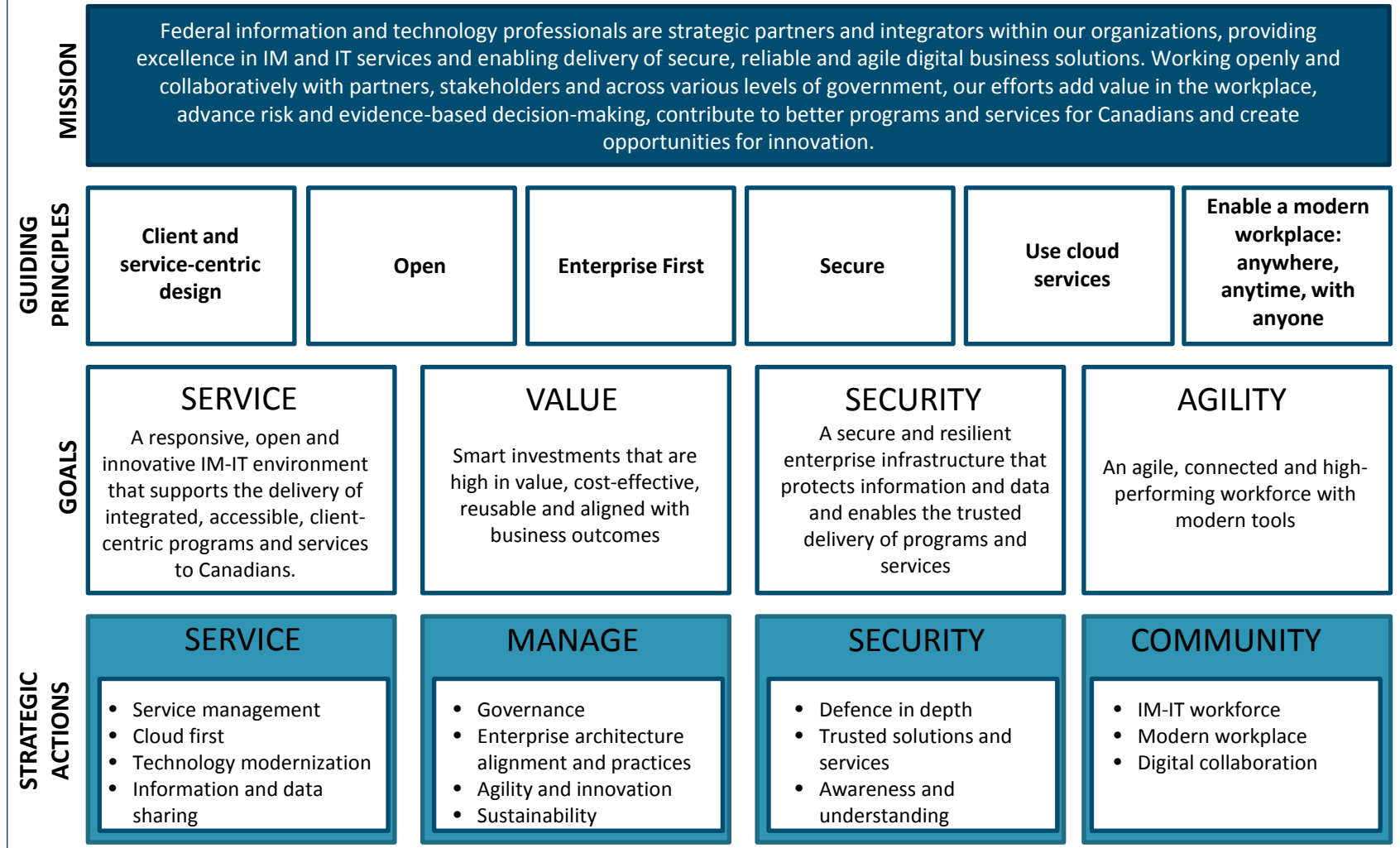
**The Government of Canada is an open and service-oriented organization that delivers programs and services to citizens and businesses in simple, modern and effective ways that are optimized for digital - available anytime, anywhere and from any device**

## Drivers

- Citizen expectations
- Workplace and workforce evolution
- Privacy and security
- The enterprise approach
- IM-IT sustainability and aging IT

# Framework

## FRAMEWORK – STRATEGIC PLAN FOR IM-IT



# Guiding Principles

Principles guide decision-making and implementation

1

## Client and service-centric design

- Government of Canada solutions and services are designed from a client-centric and end-to-end digital service delivery perspective to increase the value they bring to clients

2

## Open

- Government of Canada information and data is open by default

3

## Enterprise first

- Departments and agencies will follow common standards, approaches and direction and use existing enterprise assets (processes, data, contracts, solutions, etc.) as accelerators

4

## Secure

- Government of Canada information is safeguarded for security, privacy, confidentiality, monitored to prevent leaks, and protected for future generations

5

## Use cloud services

- Departments and agencies will explore Anything as a Service (XaaS) cloud services before developing solutions in-house

6

## Enable a modern workplace: anywhere, anytime, with anyone

- Government of Canada strives to be an innovative organization

# Strategic Goals

Goals provide areas of focus and describe high level results

- A responsive, open and innovative IM-IT environment that supports the delivery of integrated, accessible, client-centric programs and services to Canadians

Service



- Smart investments that are high in value, cost-effective, reusable and aligned with business outcomes

Value



- A secure and resilient enterprise infrastructure that protects information and data and enables the trusted delivery of programs and services

Security



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

Agility





# Strategic Actions

- Priorities for 2018/19 are key elements that enable the shift to digital service delivery

Priority (Lead)	Strategic Actions	Overview
Stabilize legacy (SSC)	6, 35	Activities required to evergreen infrastructure and reduce risks related to aging IT, including email transformation.
Departmental application strategy and plan for Data Centre Consolidation and Cloud Adoption (Departments and SSC)	4, 7	To support data centre consolidation and cloud adoption, departments require a strategy and plan to facilitate the transition of business applications from legacy data centres to new environments.
Service management (SSC, PSPC)	1, 2, 3	Implementation of enterprise service management processes and supporting toolset for consistency across departments and improved end-to-end service delivery.
GC Interoperability (TBS-CIOB)	11	Expected outcomes resulting from improved interoperability include: Seamless information flow across jurisdictions; Cost optimizations through reuse; Increased responsiveness and agility; and Improved Reporting.
Migration to GC Identity, Credential and Access Management Service (TBS-CIOB, SSC)	22	Provides a GC-wide solution that will decrease costs, enhance the experience and efficiency of end users, improve the overall security posture of GC networks, systems and applications, and provide greater control of privacy. GC ICAM will be implemented in a phased, incremental approach over a number of years.
Open Government (TBS-CIOB)	63, 73	Open Government is about making government more accessible to everyone. This means giving greater access to government data and information to the Canadian public and the businesses community.

# Next Steps

---

- Publish the updated version on Canada.ca in October
- Discussions on the shift to digital
  - Draft Strategic Plan will be shared with CIOs, IMSOs and Heads of IT on GCConnex:  
<https://gcconnex.gc.ca/groups/profile/20866369/gc-it-strategic-plan-plan-strategique-de-la-ti-du-gc>
  - 1 day workshop – Wednesday, October 18, 2017
    - Evolving the Strategic Plan to support and enable digital
- Re-design and update the Strategic Plan for 2018-19
  - Including feedback from the workshop
  - Evolve to new Digital Strategy and align to new Digital Policy
  - Engaging more broadly
- Prepare report for the Secretary on 2016 GC IT Strategic Plan

# GC Cloud Adoption Strategy

# A sub-component of the GC IT Strategic Plan

## ***Government of Canada IT Strategic Plan (2016 -2020)***

- Outlines strategic actions to position the government to manage and use IT as a strategic enterprise asset, in agile and innovative ways, to deliver better value to government programs and services
- **Guiding principle #3:**
  - Increase use of cloud computing services
- **Strategic Plan Cloud Actions**
  - All Departments
    - Adopt cloud computing services
  - SSC
    - Establish a cloud services broker service
    - Offer public cloud services
    - Offer private cloud services



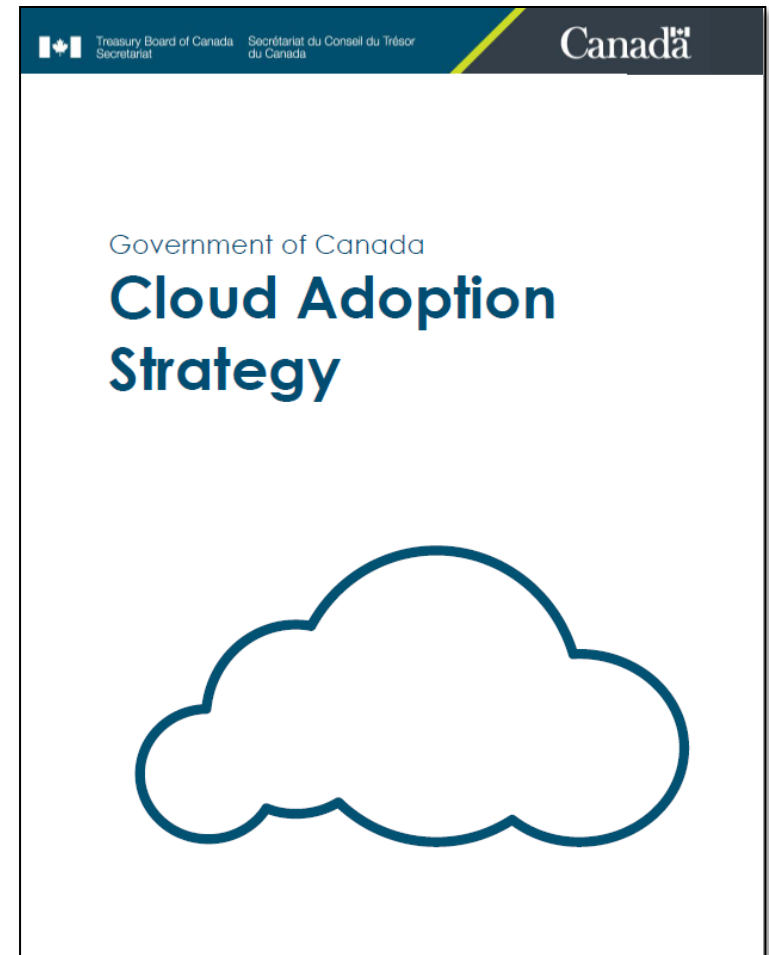
**SERVICE IT**

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

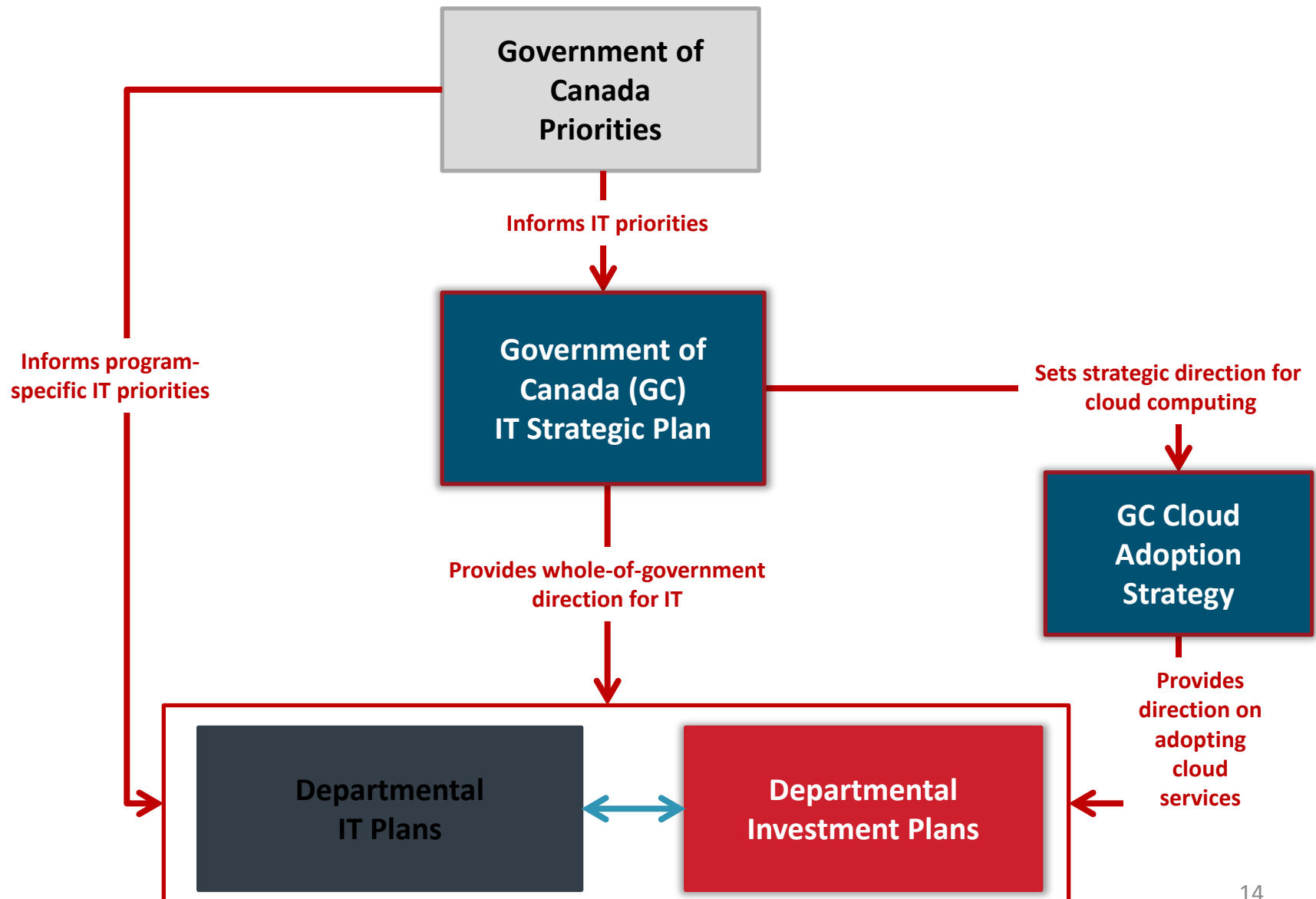
CLOUD COMPUTING	INFORMATION SHARING
<ul style="list-style-type: none"><li>• Adopt cloud computing services</li><li>• Establish a cloud service broker</li><li>• Offer public cloud services</li><li>• Offer private cloud services</li></ul>	<ul style="list-style-type: none"><li>• Build a platform for enterprise interoperability</li><li>• Introduce an enterprise mobile applications store</li><li>• Introduce a government API store</li><li>• Implement a platform for external collaboration</li><li>• Advance analytics capabilities</li></ul>

# Cloud Adoption Strategy 2017\*

- Added Hybrid Cloud and Community Cloud
- Added directional statement for Cloud First
- Expanded on Data Residency requirement for the storage of sensitive information
- Added Exit Strategy as a guiding principle before using cloud services
- Clarified roles and responsibilities between TBS, SSC, PSPC and Departments
- Other miscellaneous updates and clarifications



# Relationships between the *GC IT Strategic Plan*, SSC's Investment Plan and the *GC Cloud Adoption Strategy*



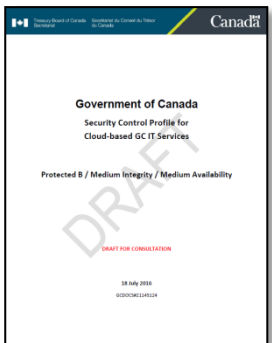
# How the GC has prepared for Cloud

*TBS has published guidance documents and is updating policy:*



**Government of Canada Cloud Adoption Strategy:** Learn how the Government of Canada will maximize the benefits of cloud adoption while keeping the confidentiality and privacy of Canadian's data.

**Government of Canada Right Cloud Selection Guidance:** Find out which workloads are right for the cloud, and how to consider deployment models.

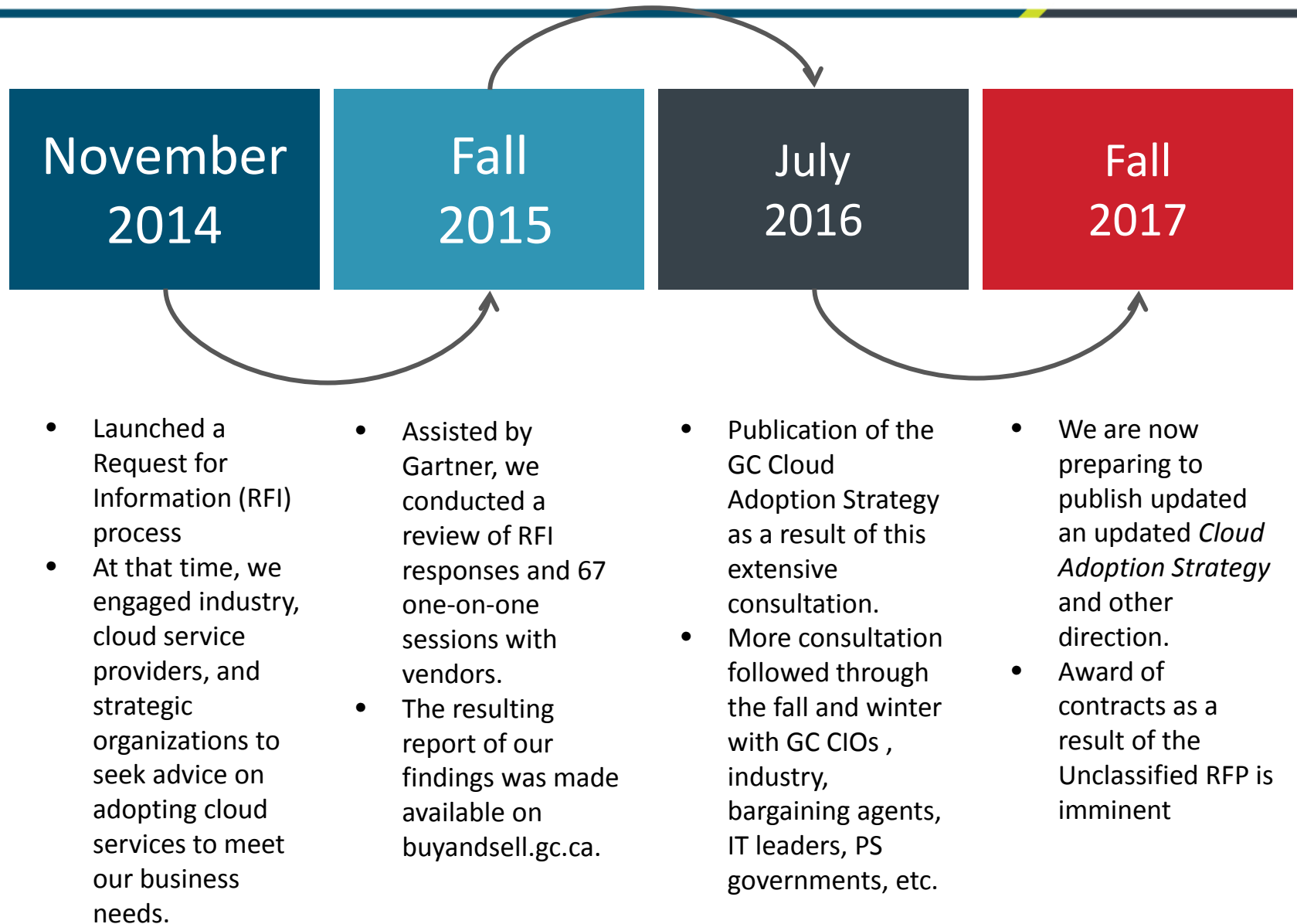


**Government of Canada Security Control Profile for Cloud-based IT Services:** A robust risk-management approach will ensure that the appropriate Government of Canada Security controls are in place.

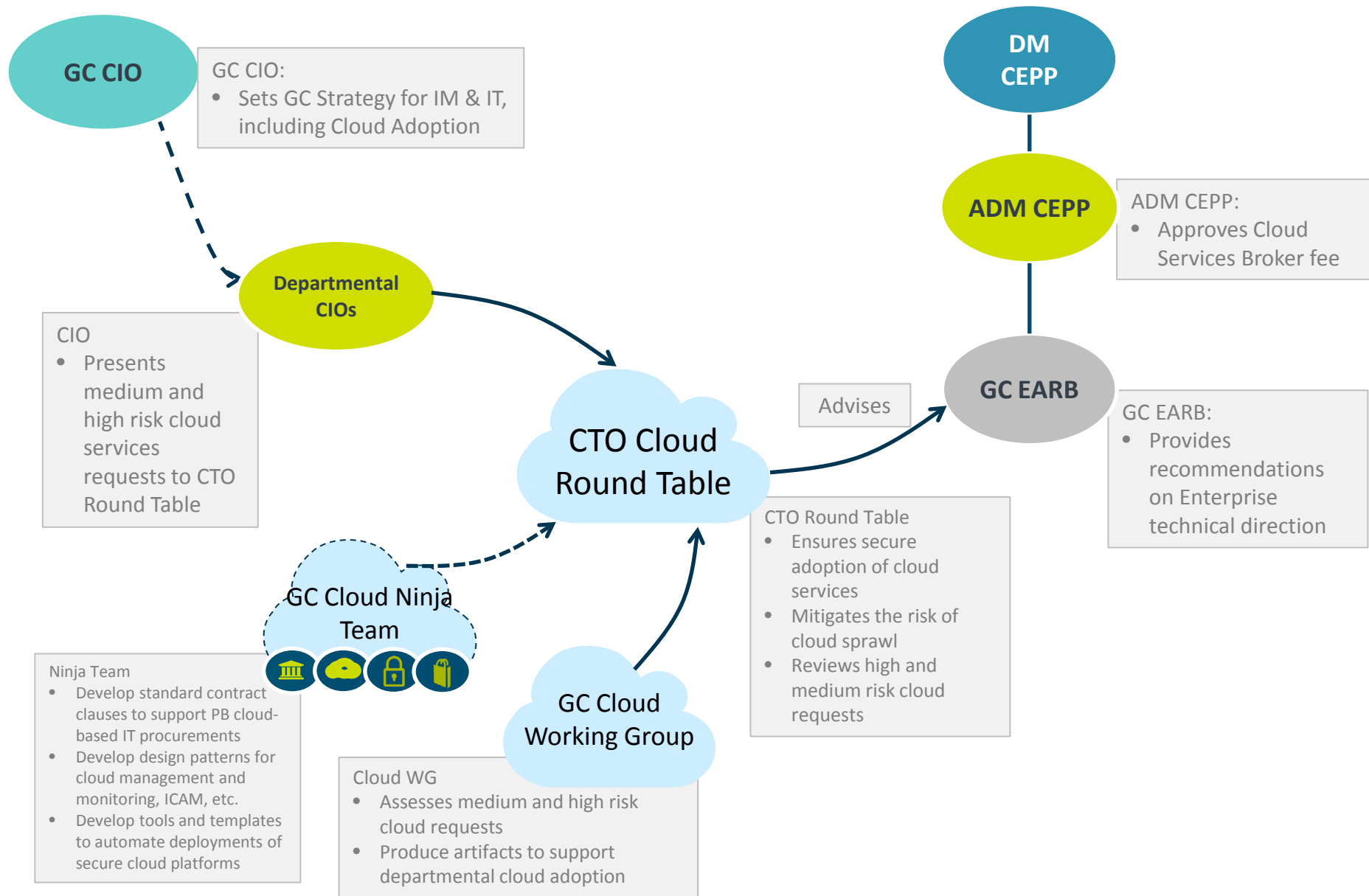




# How did we get here? GC Cloud Journey



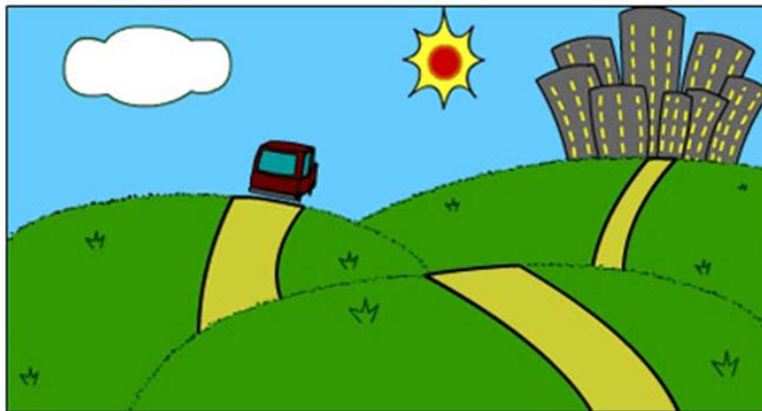
# Cloud Governance Model



# Unclassified Cloud Services Procurement

# Unclassified Cloud Services Request for Procurement

- ✓ August 2016 – Launched Invitation to Qualify (ITQ)
- ✓ Date 16, 2016 – Issued RFP to successful ITQ respondents
- ✓ June 16, 2017 – RFP Closed
- ✓ July 27, 2017 – Technical evaluations completed
- ✓ Ongoing – Perform legal due diligence on bids (Ts & Cs)
- ✓ Ongoing – Review SOC2 documentation of bidders
- ✓ September 2017 (TBC) – Begin award of contracts

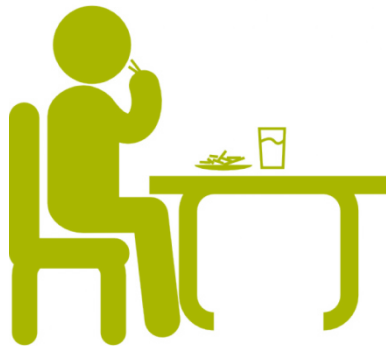


*The road has been long and bumpy but our destination is in sight!*

# Who chooses?



**Governance (Committee on Enterprise Plans & Priorities and GC EARB):** Monitors performance of the process. Provides direction on items which have been escalated.



**Departmental CIOs:** Select the appropriate option for their business context. Evaluation of the choices rest here.

Selecting the Right Cloud



**Cloud Service Broker (SSC):** Provides CIOs with procurement options to select from.

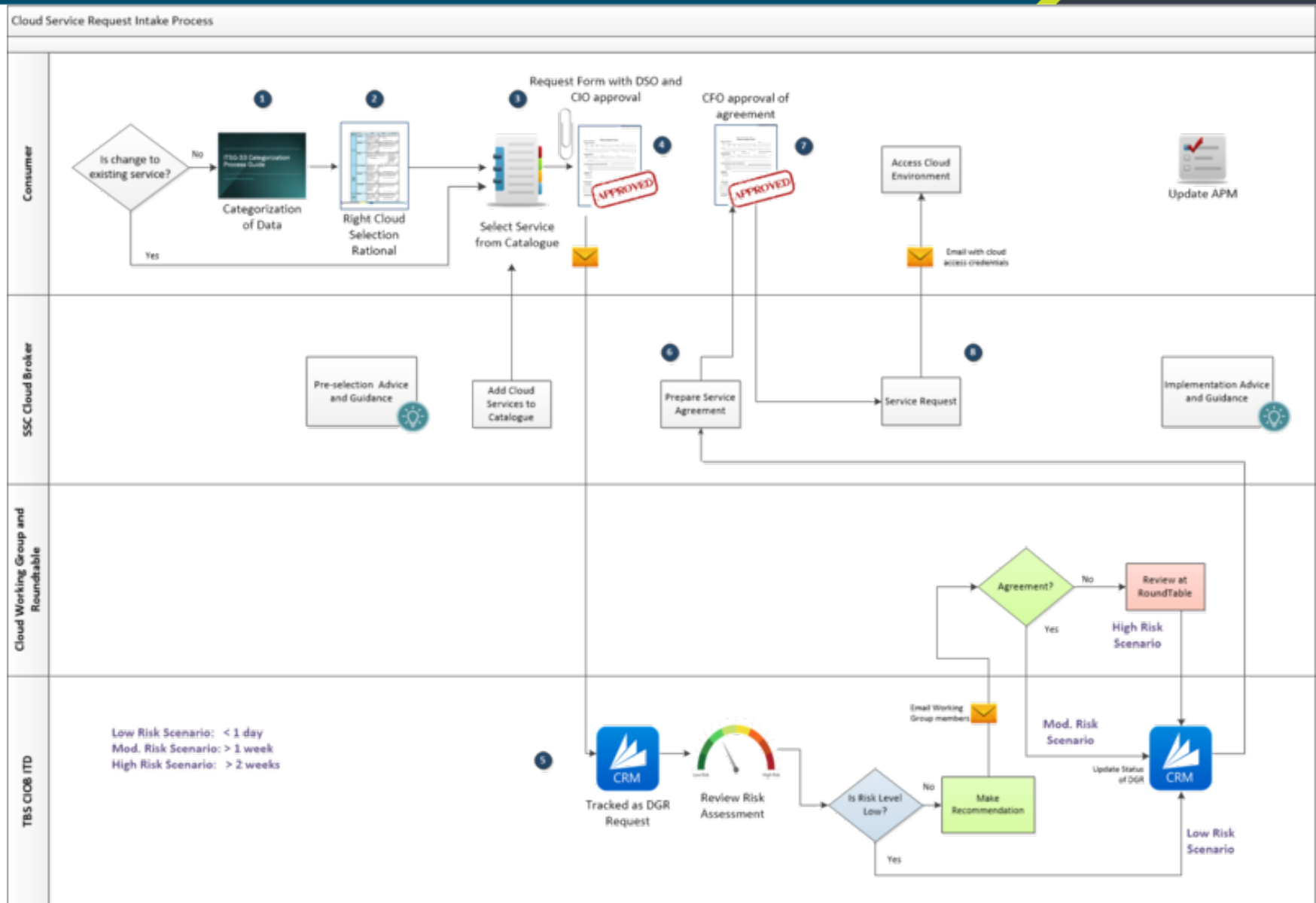


Public Cloud



Private Cloud (TBD)

# Cloud Services Intake Process



# Cloud Frequently Asked Questions (FAQs)

# Clearing up the questions

As our understanding of cloud and the myriad of cloud services available evolve, so too have misconceptions and misunderstanding among all levels.

Can the GC avoid using the Cloud?

How can I ensure my data will be safe?

Now that I have put my data in the cloud, the CSP is responsible for all security, right?



Have other countries gone "cloud first?"

Will Cloud eliminate the need for GC data centres?

Is Public Cloud Cheaper?



# GC Cloud FAQs

*The upcoming slides will highlight challenges and answer frequently asked questions related to moving protected GC services to the cloud:*

	Definition	FAQ
CLOUD FIRST	<ul style="list-style-type: none"><li>➤ A policy statement to direct all new IT projects to leverage cloud-based services (with an adequate business case for not using cloud)</li></ul>	<ul style="list-style-type: none"><li>➤ Have other governments adopted a cloud first policy?</li></ul>
DATA RESIDENCY	<ul style="list-style-type: none"><li>➤ Reference to the physical or geographical location of an organization's data (i.e. all GC data above unclassified must be stored on Canadian soil)</li></ul>	<ul style="list-style-type: none"><li>➤ Does sensitive and protected information have to reside in Canada?</li></ul>
DATA SOVEREIGNTY	<ul style="list-style-type: none"><li>➤ Concept that all digital holdings may be subject to the laws of the country in which Service Providers are Headquartered, or even where they do business.</li></ul>	<ul style="list-style-type: none"><li>➤ Do foreign governments have unfettered access to GC data stored in foreign-owned data centres hosted on Canadian soil?</li></ul>
PROCUREMENT	<ul style="list-style-type: none"><li>➤ Ability to purchase cloud-related services via traditional acquisition methods</li></ul>	<ul style="list-style-type: none"><li>➤ Do Treasury Board policies create challenges for the procurement of cloud services?</li></ul>
VISIBILITY	<ul style="list-style-type: none"><li>➤ Ability to monitor network traffic moving to/from cloud environments</li></ul>	<ul style="list-style-type: none"><li>➤ Will the use of cloud services impact the GC's visibility of network activities and data?</li></ul>
RESPONSIBILITIES	<ul style="list-style-type: none"><li>➤ Clarity around the shared nature of security and maintenance responsibilities in a cloud environment</li></ul>	<ul style="list-style-type: none"><li>➤ Do departments have any responsibility for securing and maintaining IT services in the cloud?</li></ul>

Question: Have other governments adopted a cloud first policy?

Answer: Canada is the only member of the 5 EYES countries (UK, US, Australia, New Zealand) which has not implemented a cloud first policy.

### Issues/Considerations

- The GC **does not currently have a mandated cloud first policy** (only a recommendation in the Cloud Adoption Strategy)
- DRAFT Policy on the Management of IT may include mandatory cloud-first requirements (TBD)

### Proposed Approach

- Update the GC Cloud Adoption Strategy to reflect a stronger position on Cloud First
- Approve mandatory cloud-first requirements in IT Policy Reset – *TBD*



# Data Residency

Question: Does sensitive and protected information have to reside in Canada?

Answer: Yes, as the ability to enforce Canadian legislation (such as the Privacy Act) is limited outside of Canada

## Issues/Considerations

- **GC Cloud Adoption Strategy** states that *all sensitive or protected data under government control will be stored on servers that reside in Canada*
  - However, no policy statement currently exists to reinforce this requirement
- **DRAFT IT Policy Reset** will include a mandatory data residency requirement

## Proposed Approach

- Issue IT Policy Implementation Notice (ITPIN) to reinforce requirement for data residency in Canada for sensitive information while policy suite is being approved – *September 2017*
- Approve mandatory data residency requirement in IT Policy Reset – *Fall 2017*



# Data Sovereignty

Question: Do foreign governments have unfettered access to GC data stored in foreign-owned data centres hosted on Canadian soil?

Answer: All countries have laws to gain access data, but the GC can apply measures to comply with Canadian security and privacy regulations.

## Issues/Considerations

- There is fear that putting GC data in data centres owned by foreign countries will allow foreign governments to have unfettered access to GC information, even if the data centres reside in Canada.
- Cloud service providers are experienced with addressing information requests and remaining within the bounds of the legal process (e.g. Amazon - <https://aws.amazon.com/compliance/amazon-information-requests/>).
- Controls can be implemented to mitigate the risk of access to data, but there will always be residual risks when adopting cloud services.

## Proposed Approach

- Obtain Cloud Service Providers attestation regarding their process/response to information requests – *August 2017*
- Obtain Canadian and US legal opinions on data sovereignty related to cloud – *August 2017*
- Develop data encryption strategies and guidance to provide additional protection measures for GC data (e.g. use of GC held encryption keys) to mitigate risks – *August 2017*



Question: Do Treasury Board policies create challenges for the procurement of cloud services?

Answer: Current approach to procurement creates challenges when procuring cloud-based services

## Issues/Considerations

- The GC currently procures cloud using current contract clauses that were designed for on-premise deployments and commodity groups for goods and professional services, not cloud-based services.
- Security validation related to personnel screening, site (facility) clearances and supply chain integrity is also based on traditional approaches.
- The GC needs a consistent and streamlined procurement process that supports the delivery of cloud services in a timely fashion while maintaining the security posture of the GC

## Proposed Approach

- Approval of Security Policy Implementation Notice (SPIN) to clarify direction related to facilities/personnel security requirements for cloud-based services (leveraging industry standards where possible) – *September 2017*
- Evolve procurement process to establish commodity groups for cloud-based services and establish cloud-friendly standard contract clauses aligned with industry approaches (e.g. ISO27001, ISO27017, ISO27018, etc.) – *October 2017*

Question: Will the use of cloud services impact the GC's visibility of network activities and data?

Answer: With the right architecture in place, GC visibility will be no different than it is today.

### Issues/Considerations

- Today, the GC has visibility to most traffic on the GC network via SSC/CSE. There is fear that the GC will lose visibility as services are moved to the cloud.
- Cloud service providers have mechanisms to allow GC to review and consume logs from the GC portion of cloud services that will enable support for data inspection capabilities and support for GC security monitoring and incident management.
- The GC Enterprise Architecture must evolve to implement cloud-based defensive services as part of a holistic and integrated solution that ensures visibility of GC network traffic is maintained.

### Proposed Approach

- Develop a secure cloud architecture (approved by GC Enterprise Architecture Review Board) that enables visibility of network traffic to and from GC cloud services and supports GC security monitoring and incident management – *October 2017*

Question: Do departments have any responsibility for securing and maintaining IT services in the cloud?

Answer: Cloud security is a shared responsibility between cloud service providers and departments.

## Issues/Considerations

- Departments are responsible for securing and maintaining services **IN, TO and FROM**, the cloud, while cloud service providers are responsible for security **OF** the cloud. Departments can meet some requirements by using GC provided services (e.g. SSC SOC).
- The Cloud ninja team\* has been established with key stakeholders within SSC, TBS, CSE to develop guidance (i.e. "Directive on Protected Cloud") for departments to securely implement Protected B cloud workloads.
- GC Cloud Broker has a role to play in establishing cloud contracts with the right security clauses and includes leveraging of third-party audits and industry standards and certifications.

## Proposed Approach

- Develop Protected B Cloud Directive to guide departments in deploying secure cloud services – *Ongoing (target for finalization: Fall 2017 )*
- Validate Directive with cloud pathfinder projects – *Ongoing*
- Continue evolving the GC Cloud Broker role to ensure security is considered in the processes - *Ongoing*

\*See Annex B for all members of Cloud Ninja Team

# Excerpt of draft SPIN

## 6.1.1 Security Categorization

Before using cloud services to support departmental programs, services and activities, or to hold departmental information, departments must ensure that information is identified and categorized based on the degree of injury that could be expected to result from a compromise of its confidentiality, availability or integrity. A [security categorization tool](#) is available to support departments in performing this activity.

## 6.2 Information Assurance and Asset Protection

Departments that use cloud services must safeguard their information and assets from unauthorized access, use, disclosure, modification, disposal, transmission, or destruction throughout their lifecycle. These safeguards must be commensurate with the security categorization of the information and assets, and must include an assurance that appropriate physical and personnel security controls are implemented.

### 6.2.2 Identity, Credential, and Access Management

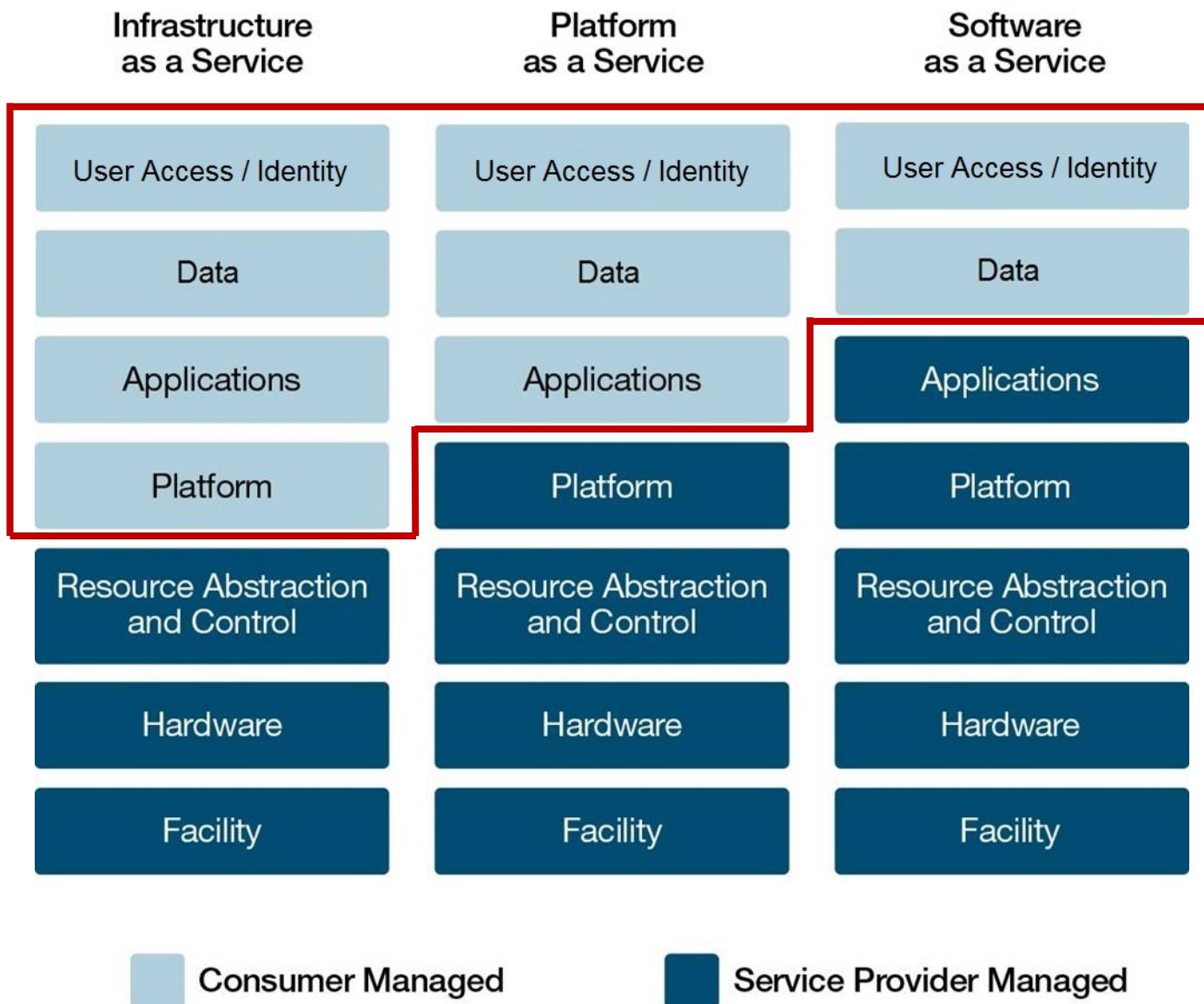
Departments are responsible for ensuring that individuals and devices are uniquely identified and authenticated to an appropriate level of assurance before being granted access to information and information systems hosted in a CSP environment, in accordance with the [Standard on Identity and Credential Assurance](#), and in alignment with GC enterprise identity and authentication services.



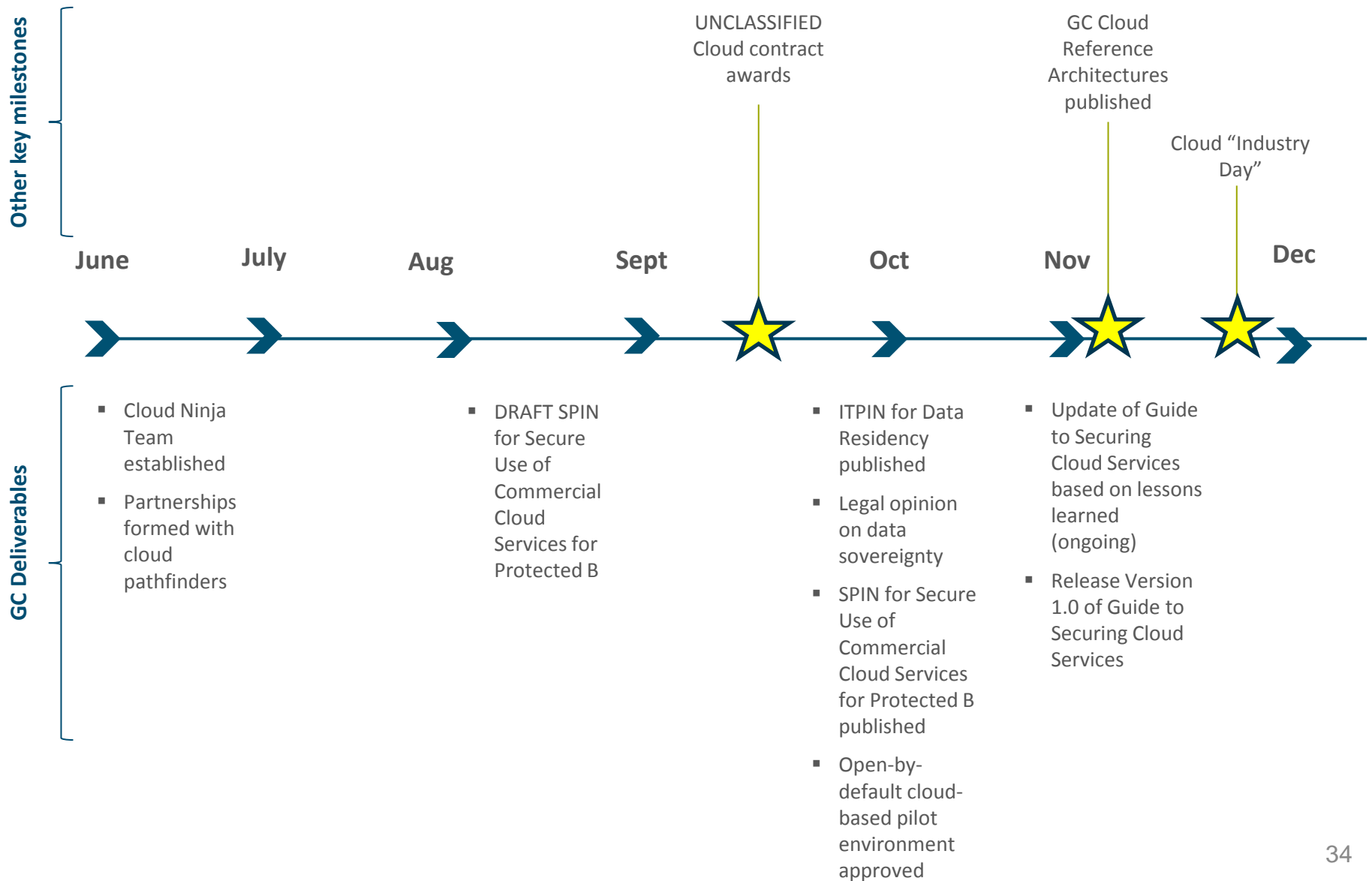


# Shared Responsibility Between GC and Cloud Service Providers

  
Departments are responsible for securing and maintaining services *IN, TO and FROM* the cloud.



# Timelines





# Additional Material GC Strategic Plan for IM & IT

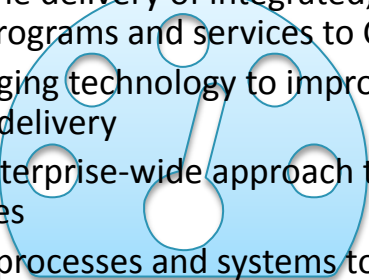
# Strategic Goals

Goals provide areas of focus and describe high level results

## Strategic Goal #1: Service

A responsive, open and innovative IM-IT environment that supports the delivery of integrated, accessible, client-centric programs and services to Canadians

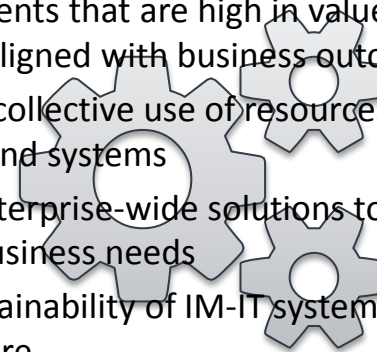
- Adopt emerging technology to improve program and service delivery
- Continue enterprise-wide approach to delivering IM-IT services
- Simplify IM processes and systems to ensure that they are effective, support objectives for openness, and relieve burden on GC workers



## Strategic Goal #2: Value

Smart investments that are high in value, cost-effective, reusable and aligned with business outcomes

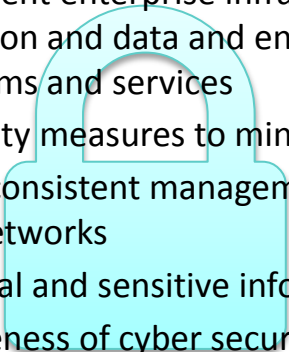
- Encourage collective use of resources, tools, processes and systems
- Develop enterprise-wide solutions to address common business needs
- Ensure sustainability of IM-IT systems and infrastructure
- Strengthen data governance and accountabilities



## Strategic Goal #3: Security

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

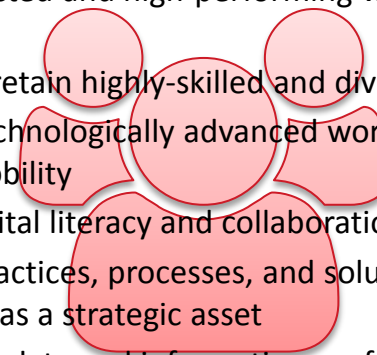
- Enhance security measures to minimize risk
- Provide more consistent management of government networks
- Protect personal and sensitive information
- Broaden awareness of cyber security risks



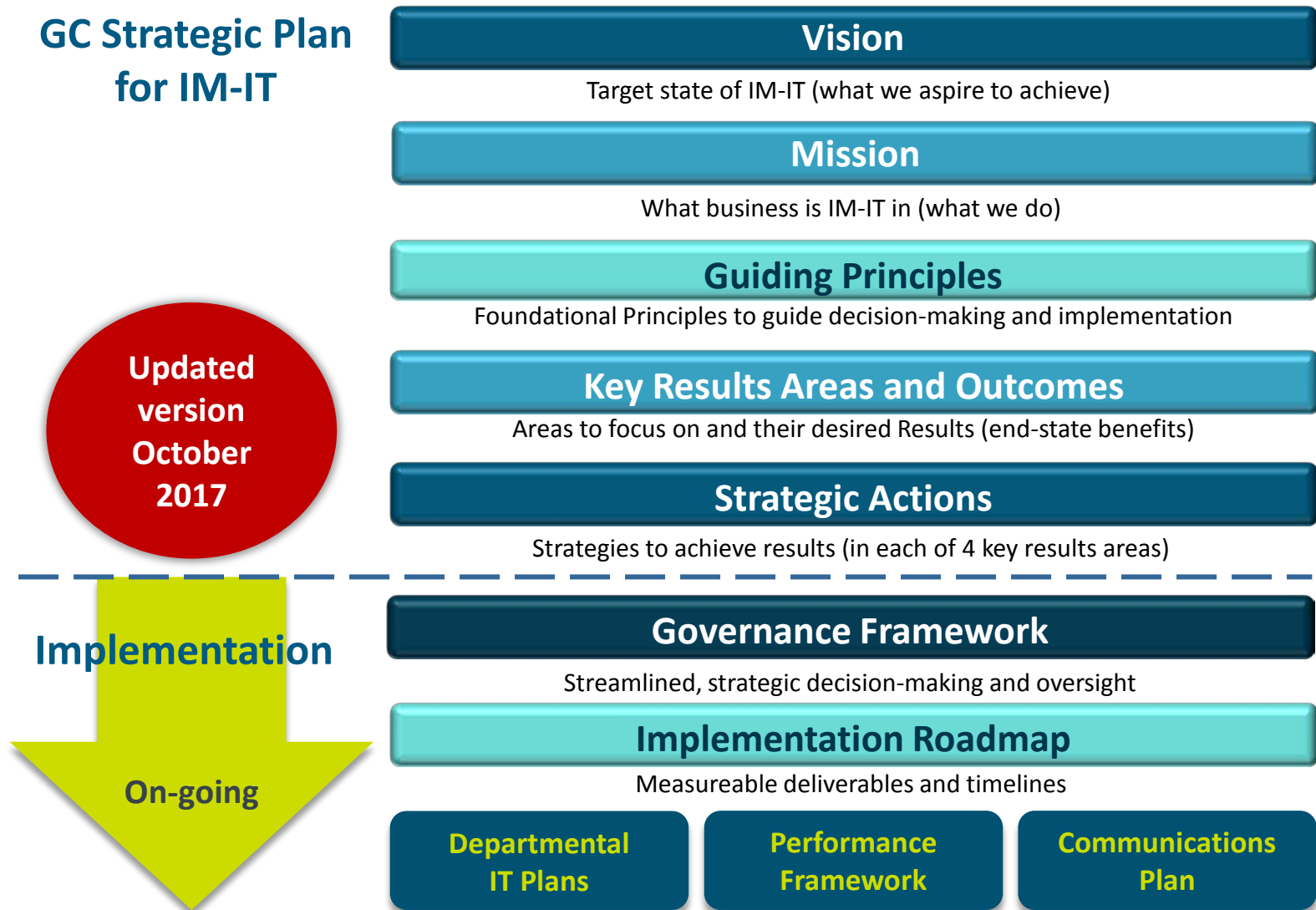
## Strategic Goal #4: Agility

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

- Attract and retain highly-skilled and diverse IM-IT talent
- Provide a technologically advanced workplace that supports mobility
- Promote digital literacy and collaboration
- Pilot new practices, processes, and solutions that exploit information as a strategic asset
- Rethink how data and information professionals can help meet current and future business needs



# Elements of the GC Strategic Plan for IM-IT



# Strategic Actions - Service



## Service management

- 1 - Develop IT service portfolios and catalogues
- 2 - Report on key areas of IT system health performance
- 3 - Implement enterprise IT service management tools
- 48 - Develop Digital Policy
- 49 - Identify and prioritize SSC essential services
- 50 - Establish SSC asset inventory and baseline

## Cloud First

- 7 - Adopt cloud services
- 8 - Establish a cloud service broker
- 9 - Offer public cloud services
- 10 - Offer private cloud services

## Technology modernization

- 4 - Complete data centre consolidation and modernization
- 5 - Complete network consolidation
- 6 - Complete government email consolidation

## Information and data sharing

- 11 - Build a platform for enterprise interoperability
- 51 - Introduce a strategy for use of open source software and open standards
- 12 - Introduce a mobile application strategy and framework
- 52 - Develop an API strategy
- 13 - Introduce a government API store
- 53 - Enhance online infrastructure to enable departments to release their data and information
- 54 - Develop master data management program
- 15 - Advance analytics
- 14 - Implement a platform for external collaboration
- 55 - Implement GCDOCS
- 56 - Migrate websites to Canada.ca



# Strategic Actions - Manage

## Governance

- 27 - Establish enterprise IM-IT governance
- 28 - Develop methods to prioritize investments in legacy and transformation initiatives
- 29 - Document roles and responsibilities for IT and IT security
- 57 - Establish data governance

## Enterprise architecture alignment and practices

- 30 - Evolve IM-IT management practices, processes and tools
- 31 - Develop enterprise architectures for business, information, applications and technology
- 32 - Adopt agile approaches to implementing business solutions
- 58 - Standardize metadata
- 59 - Develop information and data valuation framework
- 60 - Develop an information management performance framework

## Agility and innovation

- 33 - Lead innovation
- 34 - Adopt modern and flexible business models
- 61 - Create an information and data innovation engine
- 62 - Provide tools and resources to make innovative use of information and data
- 63 - Shift culture and processes toward open by design
- 64 - Establish a Digital Advisory Board
- 65 - Advance Financial Management Transformation

## Sustainability

- 35 - Ensure IT infrastructure sustainability
- 36 - Rationalize investments
- 66 - Develop process to balance infrastructure supply and demand



# Strategic Actions - Security

## Defence in depth

- 16 - Secure the government's network perimeter
- 17 - Implement endpoint security profiles
- 18 - Implement an enterprise approach to vulnerability and patch management
- 19 - Manage and control administrative privileges

## Trusted solutions and services

- 20 - Protect web transactions to and from external-facing websites
- 21 - Implement an improved cyber authentication service
- 22 - Implement a trusted digital identity for people accessing internal government networks and systems
- 23 - Implement a secure communication service for classified information
- 24 - Implement enterprise data loss prevention

## Awareness and understanding

- 25 - Enable comprehensive understanding of endpoint devices
- 26 - Enhance awareness of enterprise cyber security threat and risk environment





# Strategic Actions - Community

## IM-IT workforce

- 39 - Enable career development
- 40 - Improve diversity
- 67 - Strengthen recruitment
- 68 - Modernize information and data management profession
- 69 - Develop information and data management training
- 70 - Strengthen leadership development
- 71 - Lead targeted initiatives

## Modern workplace

- 41 - Modernize workplace technology devices
- 42 - Support a mobile workforce
- 43 - Provide Wi-Fi access
- 44 - Provide desktop videoconferencing to employees
- 45 - Implement managed print services
- 72 - Improve IM-IT accessibility

## Digital collaboration

- 46 - Promote digital literacy and collaboration
- 47 - Advance digital collaboration
- 73 - Expand open government training and outreach