Journey to Protected Cloud

Stratosphere 2019

Hello!

Bonjour!

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.

- Digital Operations Strategic Plan 2018-2022

Cloud Approach

Policy

GC Cloud Computing Direction & Standards

People

Collaborative & Skilled Community

Process

Cloud Security Risk Management, Cloud Procurement, Secure SDLC, etc.

Technology

Modern Tooling & Practices

GC CLOUD FIRST

Government of Canada   Gouvernement du Canada

Canada

Protecting Canada's Data

"…Departments must safeguard their information and assets, including those hosted in Cloud Service Provider environments, from unauthorized access, use, disclosure, modification, disposal, transmission, or destruction throughout their life cycle."

- Direction on the Secure Use of Commercial Cloud Services: SPIN 2017-01

KEY REQUIREMENTS

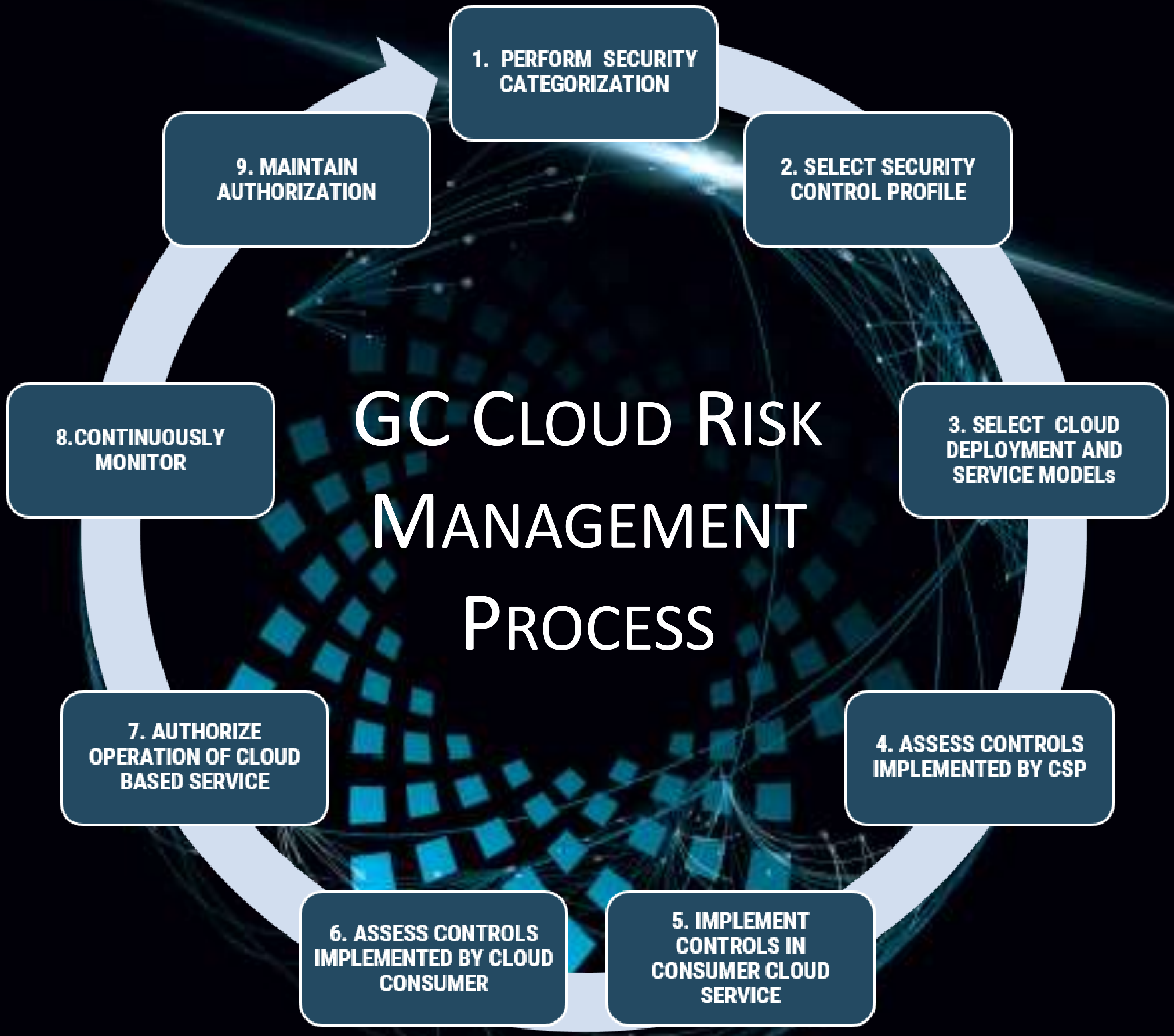
- Enable Multi-Factor Authentication
- Protect data at rest and in transit
- Manage and monitor assets and configurations
- Maintain supported software
- Patch, Patch, Patch
- Plan for breach, prepare your response plan

- Direction on the Secure Use of Commercial Cloud Services: SPIN 2017-01

Shared Responsibility Model

CSP Responsibilities + Your Responsibilities = Shared Responsibility Model

GC Cloud Risk Management Process



1. PERFORM SECURITY CATEGORIZATION

2. SELECT SECURITY CONTROL PROFILE

3. SELECT CLOUD DEPLOYMENT AND SERVICE MODELs

4. ASSESS CONTROLS IMPLEMENTED BY CSP

5. IMPLEMENT CONTROLS IN CONSUMER CLOUD SERVICE

6. ASSESS CONTROLS IMPLEMENTED BY CLOUD CONSUMER

7. AUTHORIZE OPERATION OF CLOUD BASED SERVICE

8.CONTINUOUSLY MONITOR

9. MAINTAIN AUTHORIZATION

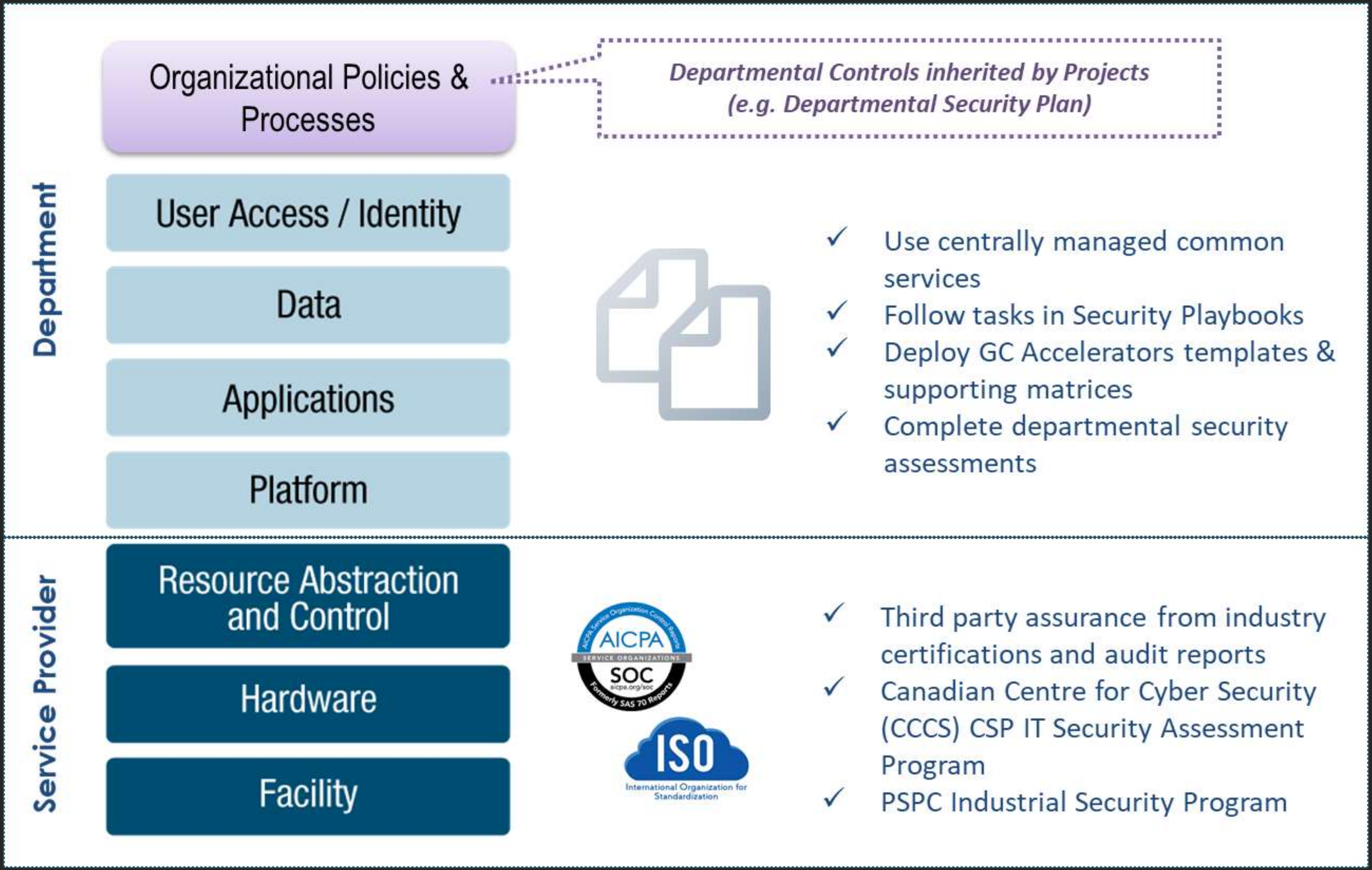
Tiered Model

Increasing levels of assurance

Requirements	Tier 0	Tier 1	Tier 2
GC Impact	Very Low	Low	Moderate
Categorization	Unclassified	Up to and including Protected A, Low Integrity, Low Availability	Up to and including Protected B, Medium Integrity, Medium Availability
Data Residency	Anywhere	Anywhere	In Canada
Location	Off-premise	Off-premise	Off-premise
Deployment Model	Public	Private, Public, Community, Hybrid	Private, Public, Community, Hybrid
Service Model	SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS

Third Party Assurance

ACCELERATE AUTHORITY TO OPERATE (ATO)



Department

Organizational Policies & Processes

Departmental Controls inherited by Projects (e.g. Departmental Security Plan)

User Access / Identity

Data

Applications

Platform

- ✓ Use centrally managed common services
- ✓ Follow tasks in Security Playbooks
- ✓ Deploy GC Accelerators templates & supporting matrices
- ✓ Complete departmental security assessments

Service Provider

Resource Abstraction and Control

Hardware

Facility

- ✓ Third party assurance from industry certifications and audit reports
- ✓ Canadian Centre for Cyber Security (CCCS) CSP IT Security Assessment Program
- ✓ PSPC Industrial Security Program

CANADIAN CENTRE FOR CYBER SECURITY

Journey to Protected B Cloud

Cyber Centre Formation and Mandate

- As of 01 Oct 2018 the Cyber Centre was stood up as part of CSE with a mandate to support the Government of Canada, industry and Canadian public.
- Prior to this CSE/Cyber Centre had been tasked by TBS in supporting PB/M/M cloud consumption as per the cloud first strategy.
- Initial efforts have been with TBS/SSC/Cyber Centre to look at security elements and how they apply to the journey of getting PB procurement of cloud for the GC – SSC to share the story of contracting next.

Cyber Centre – Where to begin?

- As per TBS efforts and direction a few specific constraints were put forth:
  - Not to reproduce FedRamp or something similar due to complexity and length of time to complete – needs to be more agile; and
  - Solutions based approach – make it as flexible as possible without sacrificing security or contravention of National Security Policies/Directives
    - Data Residency;
    - Control of information including credentials;
    - Must allow for multi-cloud instantiations; and
    - Must be ‘shareable’ and repeatable to all GC departments.
- The starting point was ITSG-33 and known baselines and existing industry standards such as ISO, and AICPA frameworks.

Cyber Centre Cloud Portfolio

- Initial work efforts were to support TBS in the review, study and development of a GC cloud security controls profile.
- This included an initial review of CSE/Cyber Centre publications and how they would need to be adapted or written to support cloud.
- Subsequently in 2018 the initial shape of the Cyber Centre Cloud portfolio started to come into focus with three branches – assessment program, advice and guidance and training and awareness.
- Branches are designed to utilize what currently exists and determine what is needed in line with TBS direction and SSC/PSPC needs at present.
- The portfolio is designed to move through ‘evolutions’ as each branch matures.

Cyber Centre Cloud Portfolio – Evolution 1

- CSP Assessment Program Development/Implementation.
- To support GC endeavours the Evolution 1 was to get an assessment program in place:
  - ITSM.50.100 developed and implemented using GC Cloud security profile.
- Program has piloted elements with different providers which have now culminated into the assessment program to support the SSC Protected B contract vehicle.
- Initially IaaS/PaaS focused; SaaS considered and being developed.

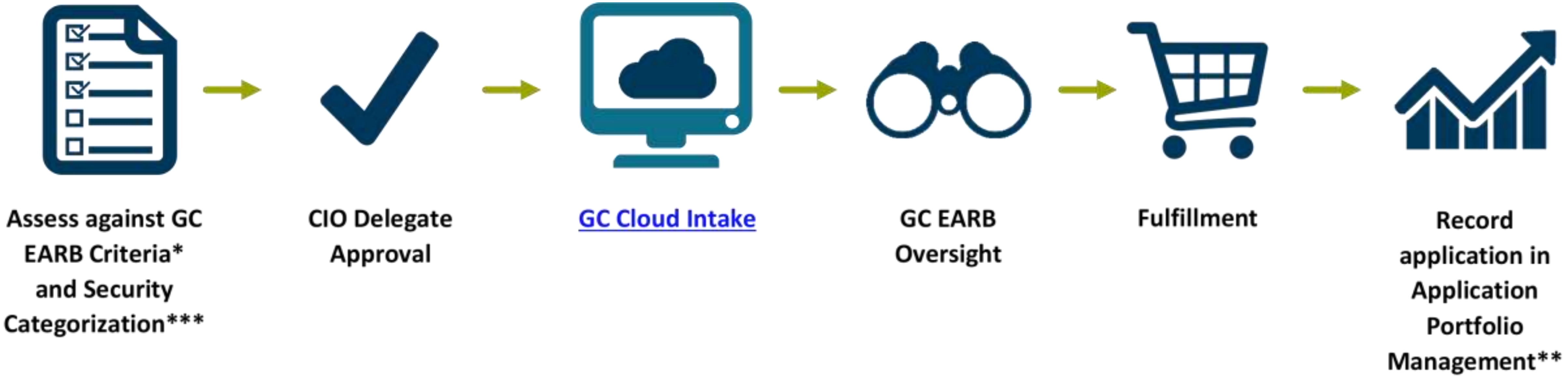
Cyber Centre Cloud Portfolio – Evolution 1

- Cornerstone Advice and Guidance publications currently in approval stages. Examples:
  - Defence In Depth (adaptations of ITSG-22 for Cloud);
  - Asset Categorization for Cloud Service Model selection;
  - Cryptographic Key Management Strategies; and
  - Cyber Centre Low/Medium Sensitivity Profiles.
- Lessons Learned documentation from Cyber Centre O365 deployment.
- Training and Awareness in discovery stages.

Cyber Centre Cloud Evolution 2

- Evolution 2 will look to CSP intake on an annual basis – not contract dependant. Estimated 2020-2021 fiscal year and will include:
  - Updated Cyber Centre profiles
    - More general language; and
    - 'Stacking' of controls listed between service models.
- Advice and Guidance to move to practitioner series for 'tenant spaces'.
- Training and Awareness to focus on specific areas not provided for by private sector training or digital training from School of Public Service.

Accessing Public Cloud Services



Assess against GC EARB Criteria* and Security Categorization***

CIO Delegate Approval

GC Cloud Intake

GC EARB Oversight

Fulfillment

Record application in Application Portfolio Management**

*Requirement 6.1.1 of the Directive on Management of IT

**Requirement 6.2.15 of the Policy on Management of IT – Will be used to assess for opportunities to increase RFSA offerings

***Requirement 6.2.7 of the Policy on Management of IT states the GC's data residency requirements

GC Cloud Brokering Service

Service de courtage infonuagique GC

GC Cloud Brokering Service

Pat Nadarajah,

Director, Cloud Brokering Services

Chief Technology Officer Branch

June 20, 2019

GC Cloud Brokering Service: Background

The GC Cloud adoption strategy originally published by TBS in 2016 and recently updated in 2018 mandated SSC to provide a light touch cloud brokering service.

“**Shared Services Canada** (SSC) is responsible for providing a light-touch cloud-brokering service by implementing contracts with cloud service providers and thereby enabling departments to use a self-service model for provisioning and managing cloud resources (for example, compute, storage, platforms).”

GC Cloud Brokering Service: Background cont'd

- Cloud Brokering Service (CBS) launched 13 Dec 2017 of Q3 FY2017-18
- 26 Contracts available to use and consume commercial public cloud services for unclassified data.
- 8 Leading Cloud Service Providers (Amazon, Microsoft, Oracle, Google, IBM, ThinkOn, OVH and Salesforce).

GC Cloud Brokering Service: Creating an Intake Process

GC Cloud Brokering Service enables clients to procure, provision, and consume approved public cloud services (unclassified data) by:

Offering Cloud Broker Strategy functions

Develop the Cloud intake process
Create cloud services supply
Handle all special requirements and facilitate the way forward
Perform trend analysis and reporting

Offering Cloud Broker Fulfillment functions:

Assists clients through cloud intake process
Assesses the cloud service requests
Coordinate the governance and approval process
Maintain and disseminate cloud service providers (CSP) service catalogues
Track and report on cloud consumption
Create consumer master accounts, to enable clients to access cloud services
Audit security policies with the customer's cloud accounting

Note: All created on the Serving Government intranet site

GC Cloud Brokering Service: Modernizing the Cloud Intake Process

In order to modernize the GC Cloud Brokering intake process SSC selected a public cloud, Customer Relationship Management (CRM) service to automate cloud service fulfillment.

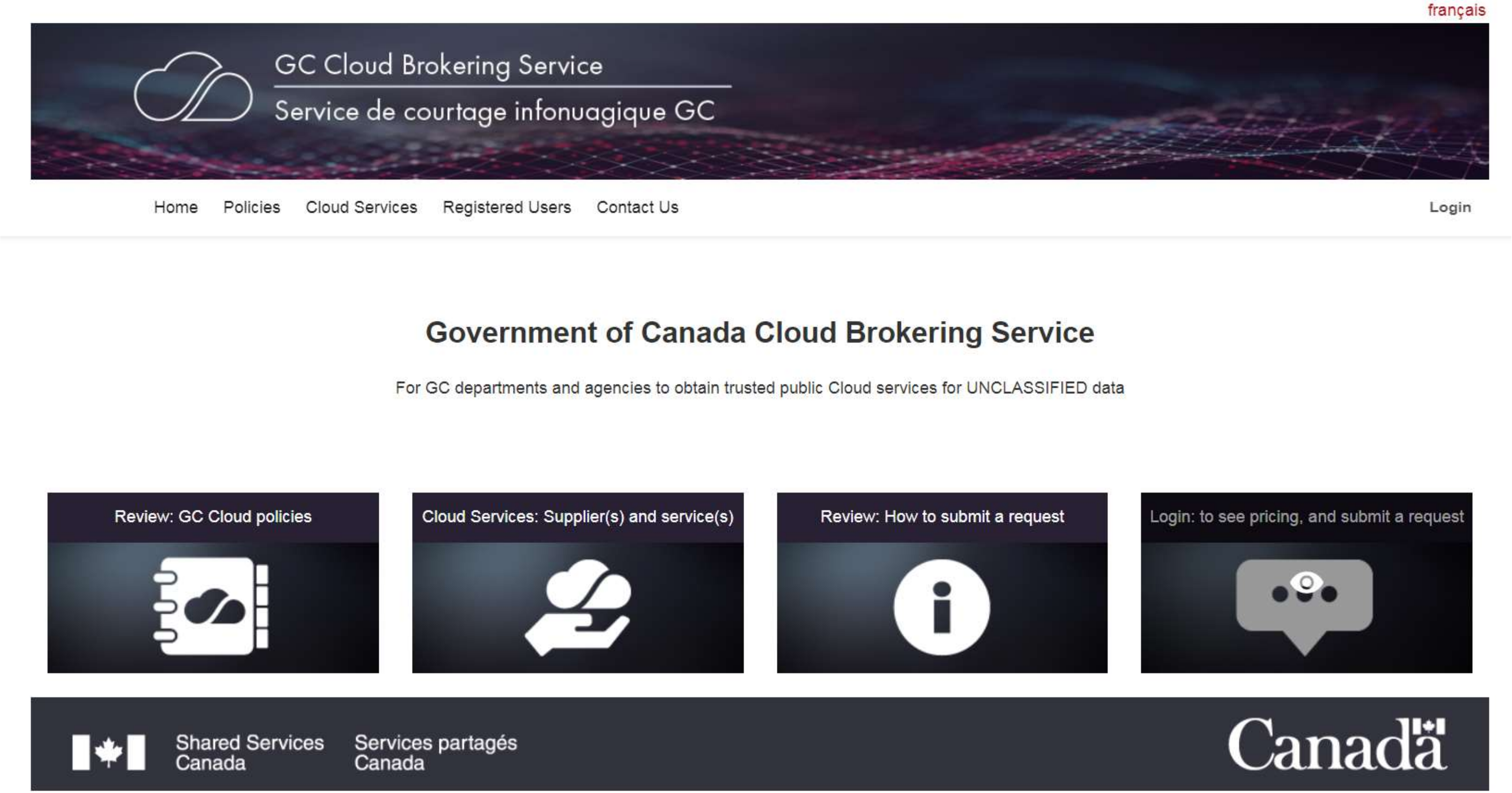
The CRM currently:

- provides an automated mechanism to submit and receive TBS/GC EARB authorization for cloud services requests.
- provides an automated capability to enforce the guardrails mandated by TBS for monitoring cloud consumption and compliance to policies
- serves as a tool to clients to track progress on their cloud services requests and provide real-time data on cloud consumption statistics and invoicing.
- serves GC clients as a single portal for cloud advisory services.
- available from desktop and through mobile services

The CRM will:

- integrate with the TBS Application Portfolio Management (APM) tool by making linkages between departmental GC IT Plans and cloud deployments.
- serve as an integration point to clients for other forms of supply, such as private cloud services, foundational services like secure connectivity and other future cloud-related services.
- Through API services give GC the ability to integrate directly with the public cloud service provider offerings.

GC Cloud Brokering Service: CRM DEMO



français

GC Cloud Brokering Service

Service de courtage infonuagique GC

Home
Policies
Cloud Services
Registered Users
Contact Us
Login

Government of Canada Cloud Brokering Service

For GC departments and agencies to obtain trusted public Cloud services for UNCLASSIFIED data

Review: GC Cloud policies
Cloud Services: Supplier(s) and service(s)
Review: How to submit a request
Login: to see pricing, and submit a request

Shared Services Canada

Services partagés Canada

Canada

Day 1…

GC Accelerators

Key Components

Design Patterns
Common designs and blueprints

Templates
Templates and tooling to enable automation

Playbooks
Guidance for GC responsibilities

Key Outcomes

AGILITY | **VISIBILITY** | **ASSURANCE**

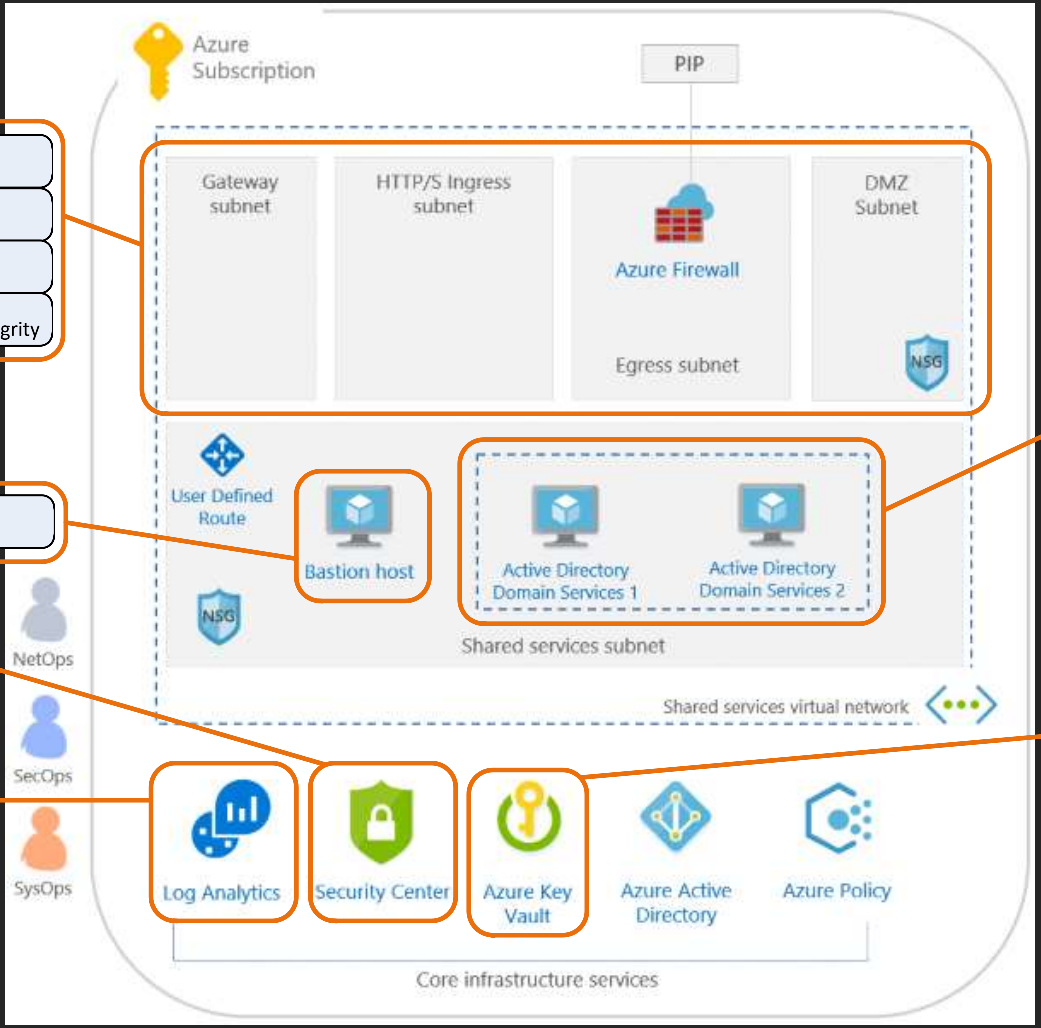
Design Patterns

AC-4	Information flow enforcement
SC-7	Boundary protection
SC-5	Denial of service protection
SC-8	Transmission confidentiality & integrity

AC-17	Remote access

RA-5	Vulnerability scanning

AU-6	Audit review, analysis, and reporting
AU-12	Audit generation
SI-4	Information system monitoring

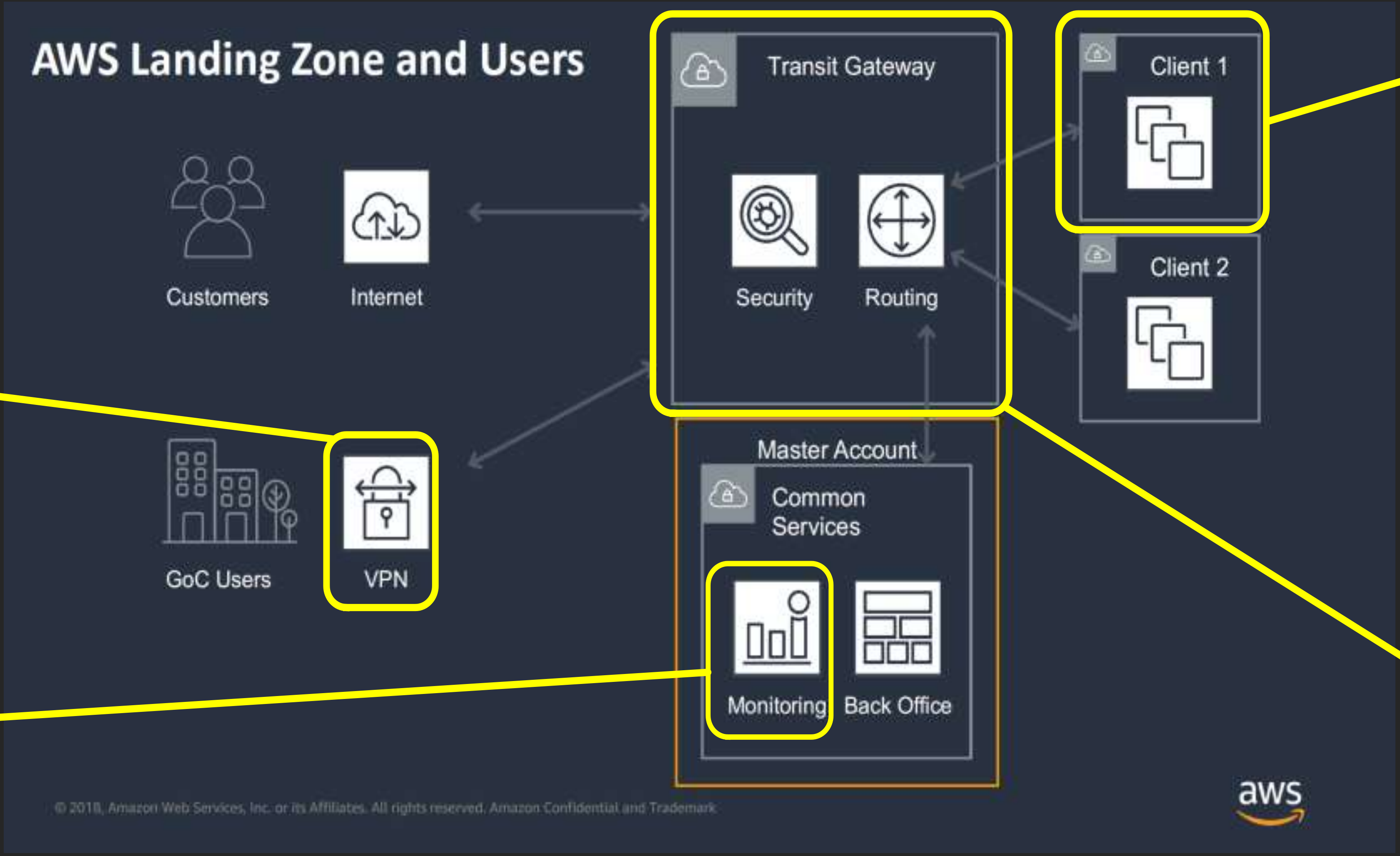


AC-2	Account management
AC-3	Access enforcement
AC-5	Separation of duties
AC-6	Least privilege
IA-2	I&A (organizational users)
IA-3	Device I&A
IA-4	Identifier management
IA-5	Authenticator management
IA-8	I&A (non-organizational users)
IA-9	Service I&A

SC-12	Crypto key establishment & management
SC-13	Cryptographic protection
SC-17	PKI certificates

https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared/

Design Patterns


AWS Landing Zone and Users
Transit Gateway
Security
Routing
Client 1
Client 2
Customers
Internet
GoC Users
VPN
Master Account
Common Services
Monitoring
Back Office
© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark
aws

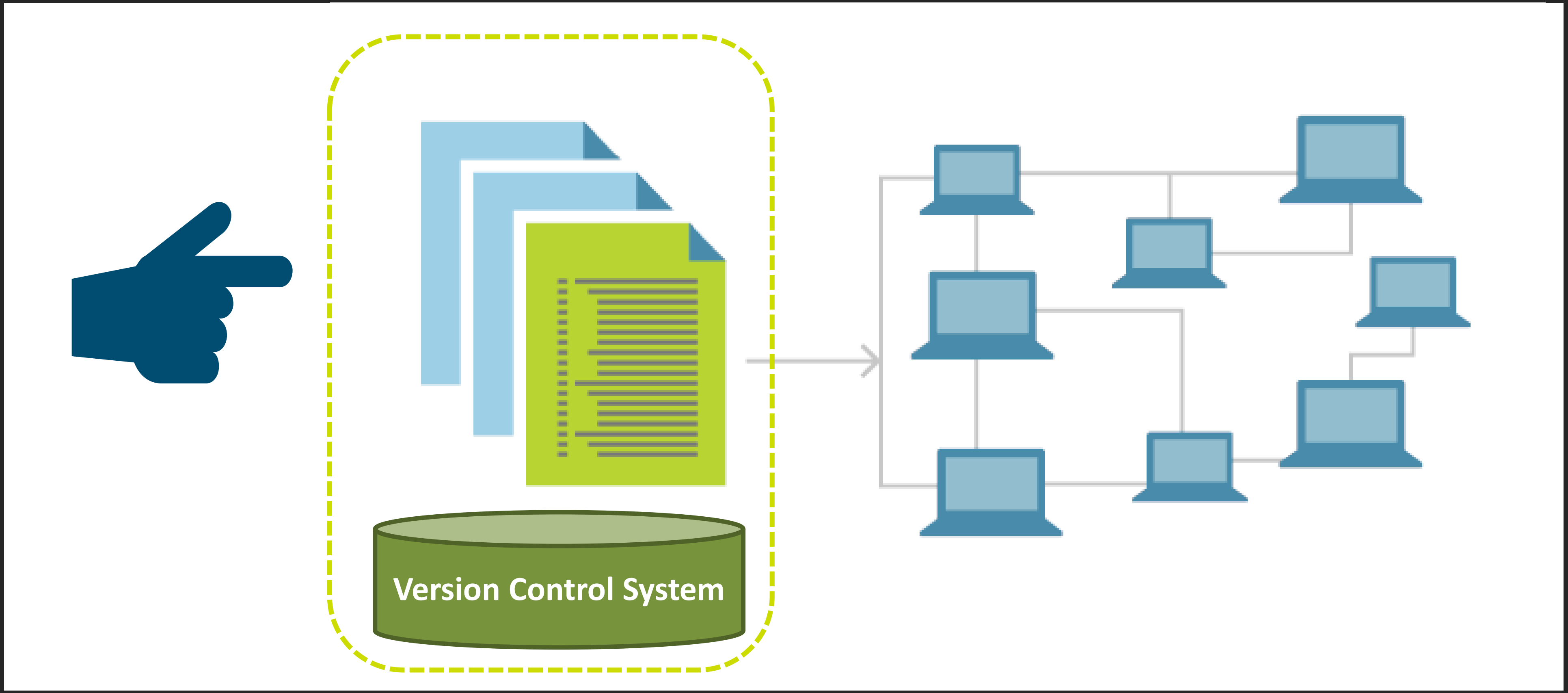
AC-17	Remote access

SI-4	Information system monitoring

AC-2	Account management
AC-3	Access enforcement
AC-5	Separation of duties
AC-6	Least privilege
AU-6	Audit review, analysis, and reporting
AU-12	Audit generation
IA-2	I&A (organizational users)
IA-4	Identifier management
IA-5	Authenticator management
IA-8	I&A (non-organizational users)
IA-9	Service I&A
SC-8	Protection of Information at Rest

AC-4	Information flow enforcement
AU-12	Audit generation
SC-7	Boundary protection
SC-5	Denial of service protection
SC-8	Transmission confidentiality & integrity

Infrastructure as Code....



....Security as Code

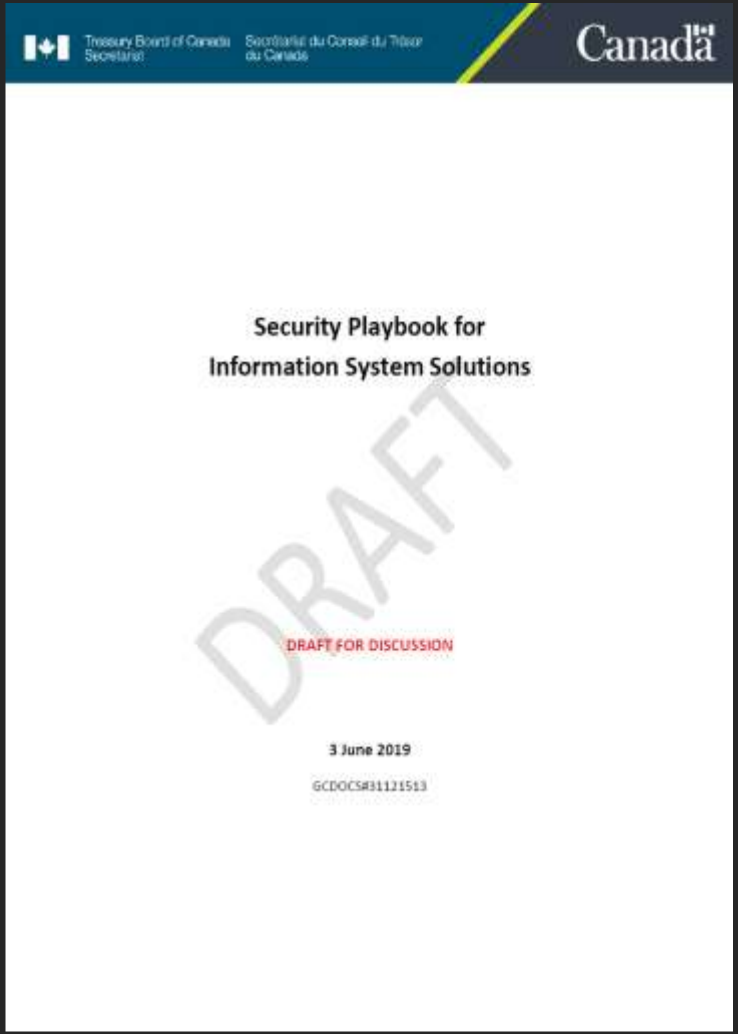
https://github.com/canada-ca/accelerators_accelerateurs-azure

https://github.com/canada-ca/accelerators_accelerateurs-aws
(in progress)

PLAYBOOKS

Key activities and tasks for Projects

- Security categorization
- System concept
- Identity and access management
- Auditing
- Data protection
- Networking
- Secure development
- Service continuity
- Configuration management
- Security operations



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

Canadä

Security Playbook for
Information System Solutions

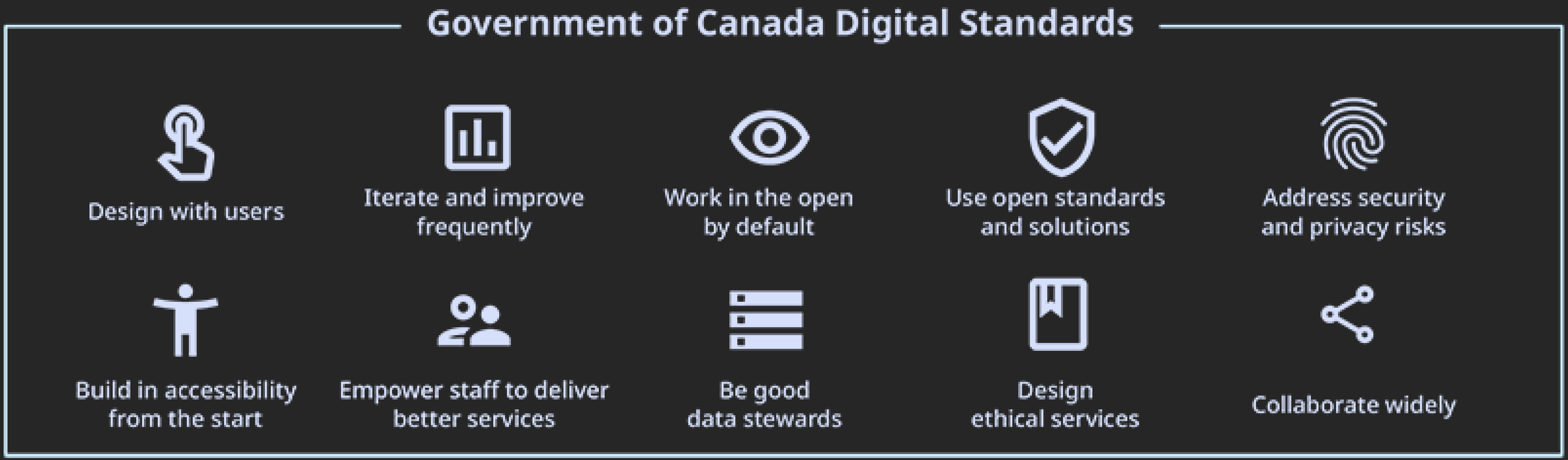
DRAFT FOR DISCUSSION

3 June 2019

GCDOCS#31121513

Check out the draft!
https://docs.google.com/document/d/1-SD7KgoRRcYN-l_HAsI_uYTjuwN899PN0RcxhjcJ9JE/edit?usp=sharing

Start with one application



Government of Canada Digital Standards

- Design with users
- Iterate and improve frequently
- Work in the open by default
- Use open standards and solutions
- Address security and privacy risks
- Build in accessibility from the start
- Empower staff to deliver better services
- Be good data stewards
- Design ethical services
- Collaborate widely

Which one will you choose?

Thank you!

TBS-OCIO, Cyber Security
ZZTBSCYBERS@tbs-sct.gc.ca

Canadian Centre for Cyber Security
contact@cyber.gc.ca

SSC Cloud Broker
ssc.cloud-infonuagique.spc@canada.ca

Annex

References

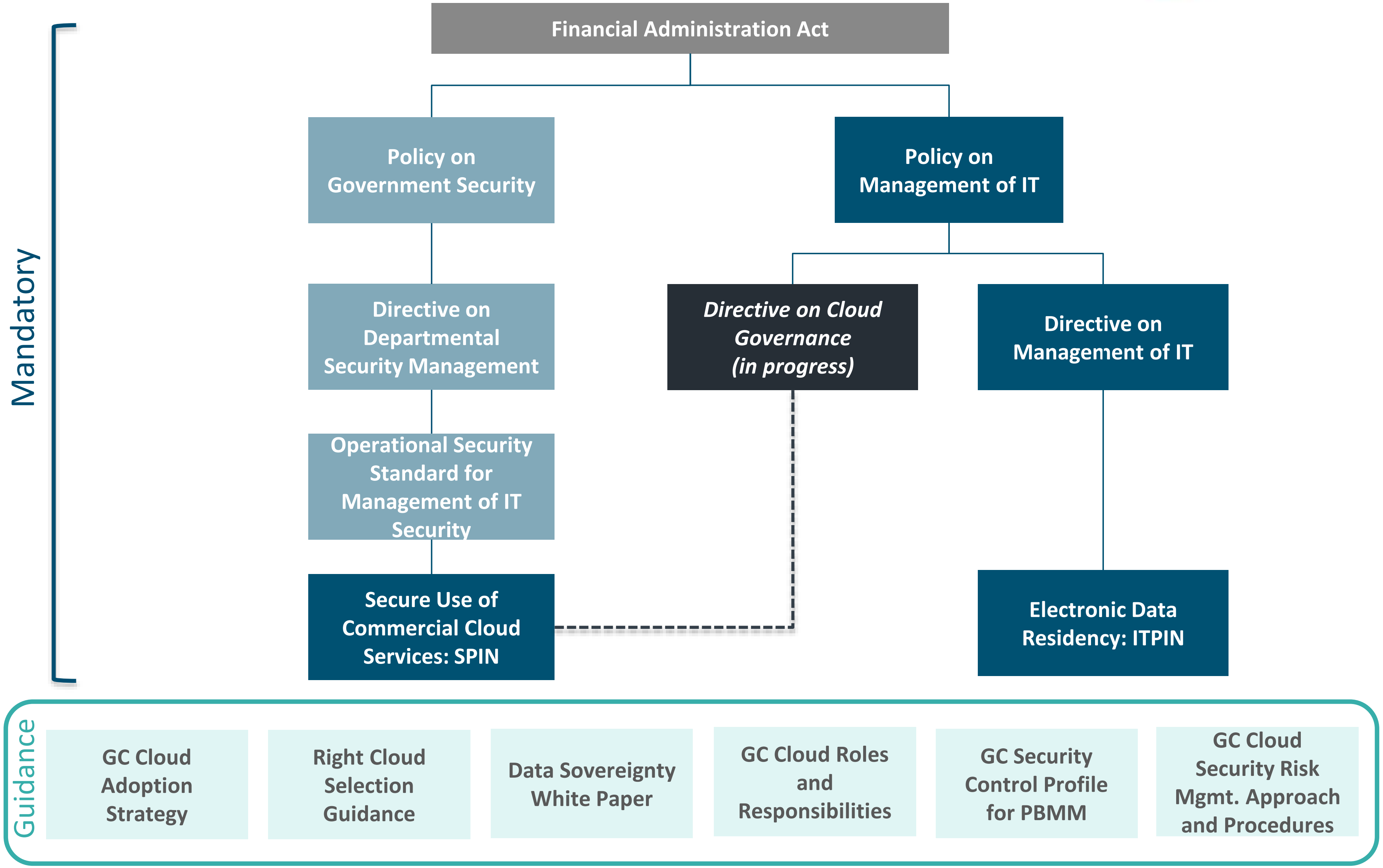
TB Policies & Standards

- Policy on Management of Information Technology
- Policy on Government Security
- Direction for Electronic Data Residency, ITPIN No: 2017-02
- Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)

Guidance

- Government of Canada Security Control Profile for Cloud-Based GC IT Services
- Government of Canada Cloud Security Risk Management Approach and Procedures
- CSE ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada
- CSE ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones
- CSE ITSP.30.031 V2 User Authentication Guidance for Information Technology Systems
- CSE ITSP.40.062 Guidance on Securely Configuring Network Protocols

Cloud Policy Architecture



Mandatory

Financial Administration Act

Policy on Government Security

Directive on Departmental Security Management

Operational Security Standard for Management of IT Security

Secure Use of Commercial Cloud Services: SPIN

Policy on Management of IT

Directive on Cloud Governance (in progress)

Directive on Management of IT

Electronic Data Residency: ITPIN

Guidance

GC Cloud Adoption Strategy

Right Cloud Selection Guidance

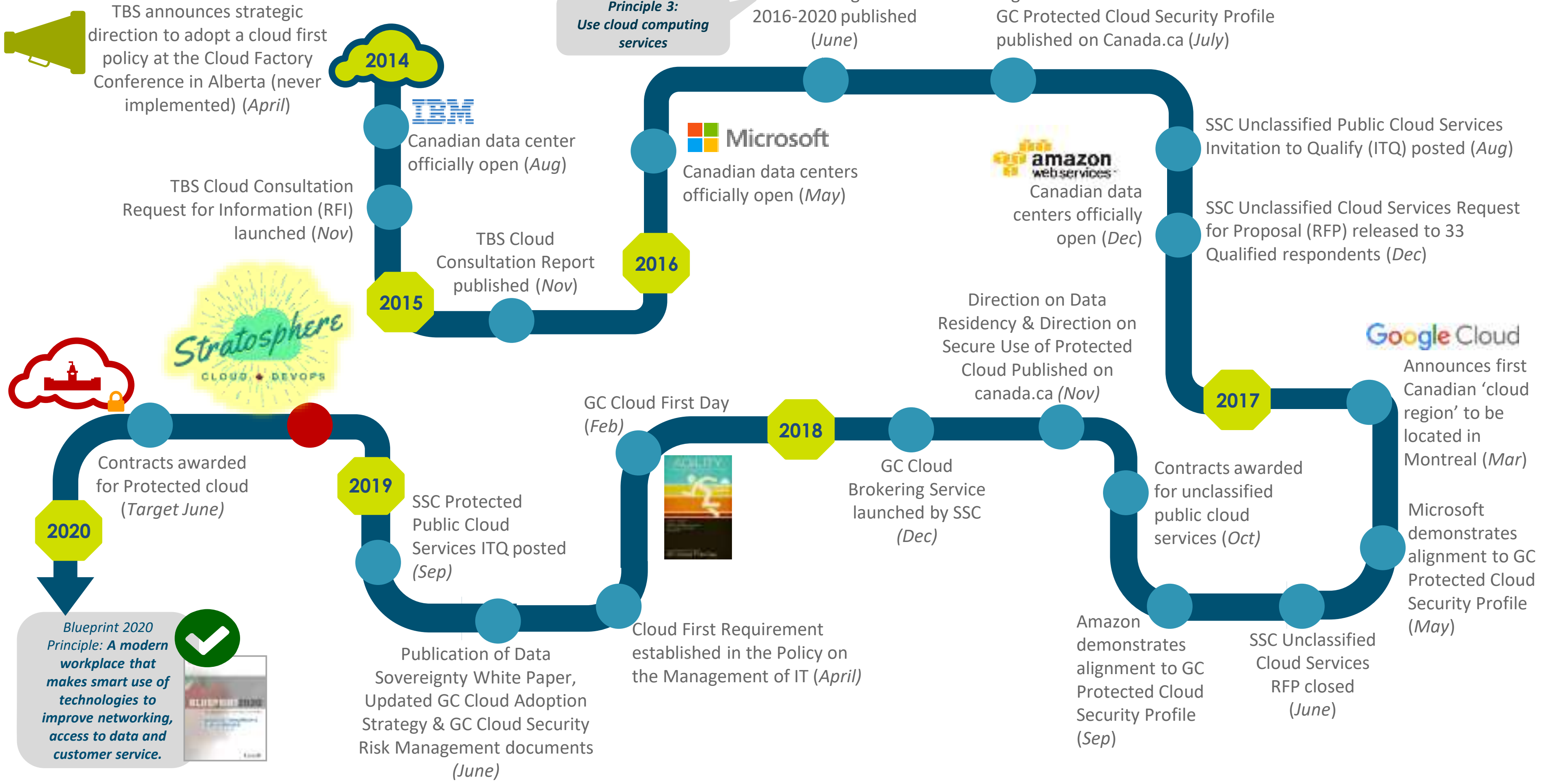
Data Sovereignty White Paper

GC Cloud Roles and Responsibilities

GC Security Control Profile for PBMM

GC Cloud Security Risk Mgmt. Approach and Procedures

The GC Cloud Journey



TBS announces strategic direction to adopt a cloud first policy at the Cloud Factory Conference in Alberta (never implemented) (*April*)

Canadian data center officially open (*Aug*)

TBS Cloud Consultation Request for Information (RFI) launched (*Nov*)

TBS Cloud Consultation Report published (*Nov*)

Canadian data centers officially open (*May*)

***Principle 3:* Use cloud computing services**

GC IT Strategic Plan 2016-2020 published (*June*)

GC Cloud Adoption Strategy, Right Cloud Selection Guidance and GC Protected Cloud Security Profile published on Canada.ca (*July*)

SSC Unclassified Public Cloud Services Invitation to Qualify (ITQ) posted (*Aug*)

Canadian data centers officially open (*Dec*)

SSC Unclassified Cloud Services Request for Proposal (RFP) released to 33 Qualified respondents (*Dec*)

Announces first Canadian 'cloud region' to be located in Montreal (*Mar*)

Microsoft demonstrates alignment to GC Protected Cloud Security Profile (*May*)

SSC Unclassified Cloud Services RFP closed (*June*)

Amazon demonstrates alignment to GC Protected Cloud Security Profile (*Sep*)

Contracts awarded for unclassified public cloud services (*Oct*)

Direction on Data Residency & Direction on Secure Use of Protected Cloud Published on canada.ca *(Nov)*

GC Cloud Brokering Service launched by SSC *(Dec)*

GC Cloud First Day (*Feb*)

Cloud First Requirement established in the Policy on the Management of IT (*April*)

Publication of Data Sovereignty White Paper, Updated GC Cloud Adoption Strategy & GC Cloud Security Risk Management documents *(June)*

SSC Protected Public Cloud Services ITQ posted *(Sep)*

Contracts awarded for Protected cloud (*Target June*)

Blueprint 2020 Principle: ***A modern workplace that makes smart use of technologies to improve networking, access to data and customer service.***