

Enabling Secure #GCDigital

A Continuous Security Approach

Presentation by Po Tea-Duncan
A/Executive Director, Cyber Security Division
Office of the Chief Information Officer
Government of Canada

- 1 The Context
- 2 The Cyber Security Landscape
- 3 Continuous Security
- 4 Digital Identity



A conceptual image featuring a human hand in a dark suit sleeve holding a glowing, translucent circuit board. The board is covered in a complex pattern of white lines and dots, resembling a microchip or data network. The background is a solid dark teal color. The text "The Context" is centered in white, sans-serif font.

The Context

Laying the digital foundation



*“The new Policy on Service and Digital sets the **foundation for the future of digital government** in Canada. We’re doing the hard work behind the scenes to set in place the conditions for **truly client-centered service design and delivery**, and to **deliver better services to Canadians**.”*

The Honorable Joyce Murray,
Minister of Digital Government (2 August 2019)



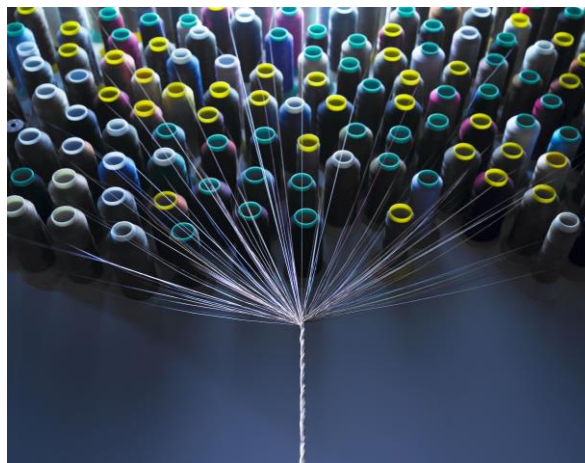
Building a vision for delivering services that are secure, accessible and easy to use



Transform

Transform **how government does business** by:

- Managing and protecting data and information
- Being open and transparent
- Leveraging new technology to improve operations and service delivery



Consolidate

Consolidate several existing policy instruments into a **single set of rules and guidelines** for the **integrated management** of:

- Service delivery
- Information and data
- Technology and cyber security



Maintain pace with change

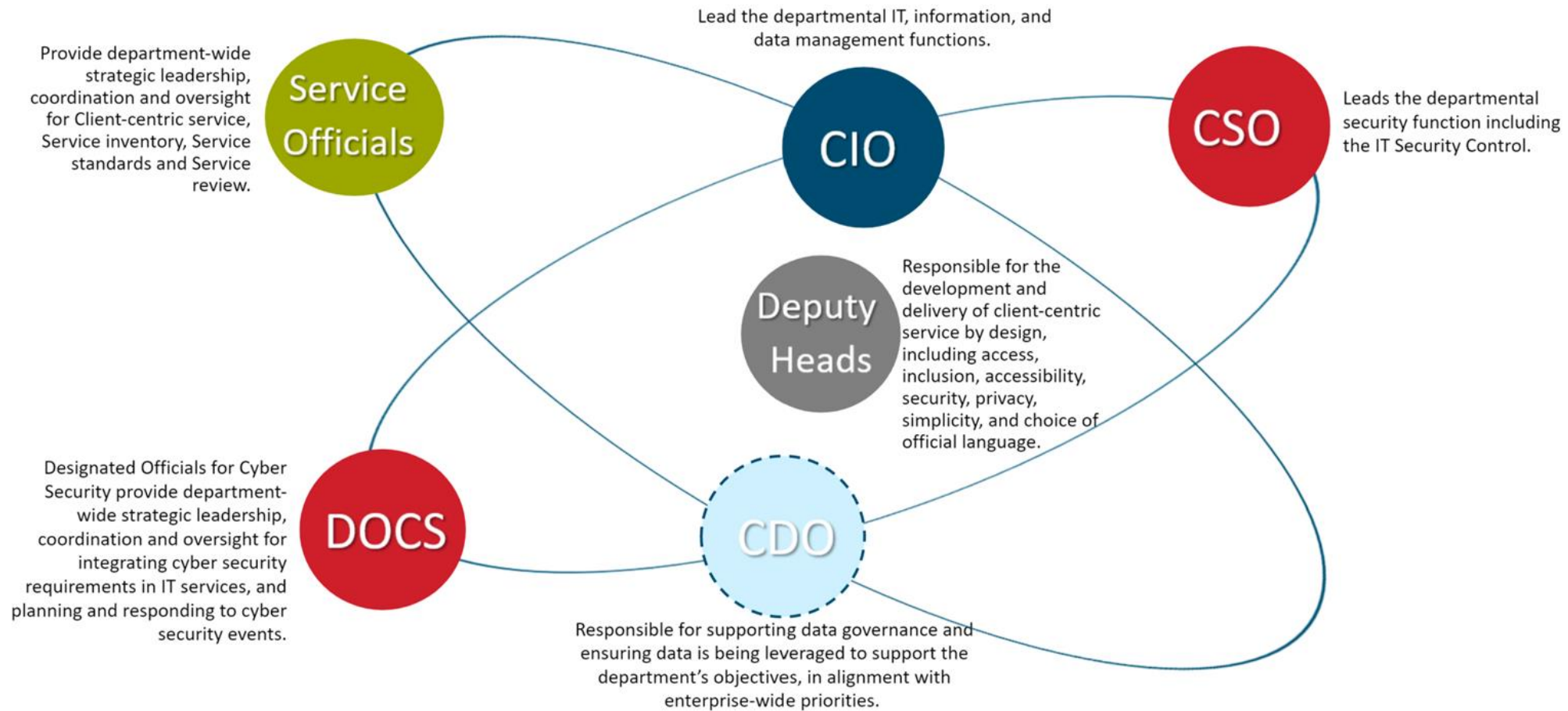
Enables the Government of Canada to **maintain pace with change in the digital era** through the responsible use of delegated authorities

Treasury Board Policy Framework

The IT security control under the Policy on Government Security is operationalized under the Policy on Service and Digital.



Working together to improve cyber security



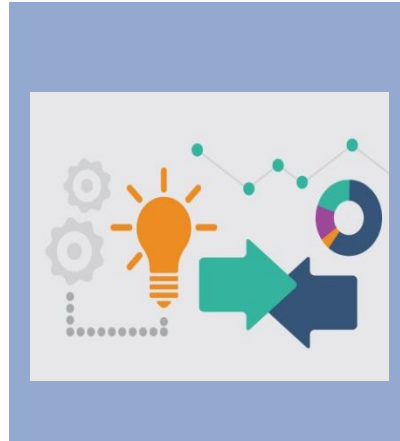
Key Stakeholders



NATIONAL

Public Safety DND
CSIS CSE
RCMP

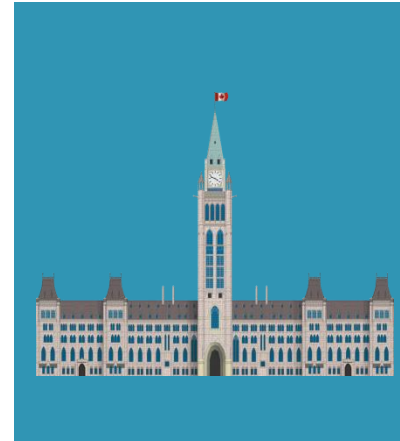
Federal government departments with responsibilities for national cyber security



SPECIALIZED

GAC ISED
PSPC DRDC
PCO CRTC

Federal government departments with specialized responsibilities for cyber security



GOVERNMENT-WIDE

TBS
CSE/CCCS
SSC

Federal government departments with responsibilities for government-wide cyber security

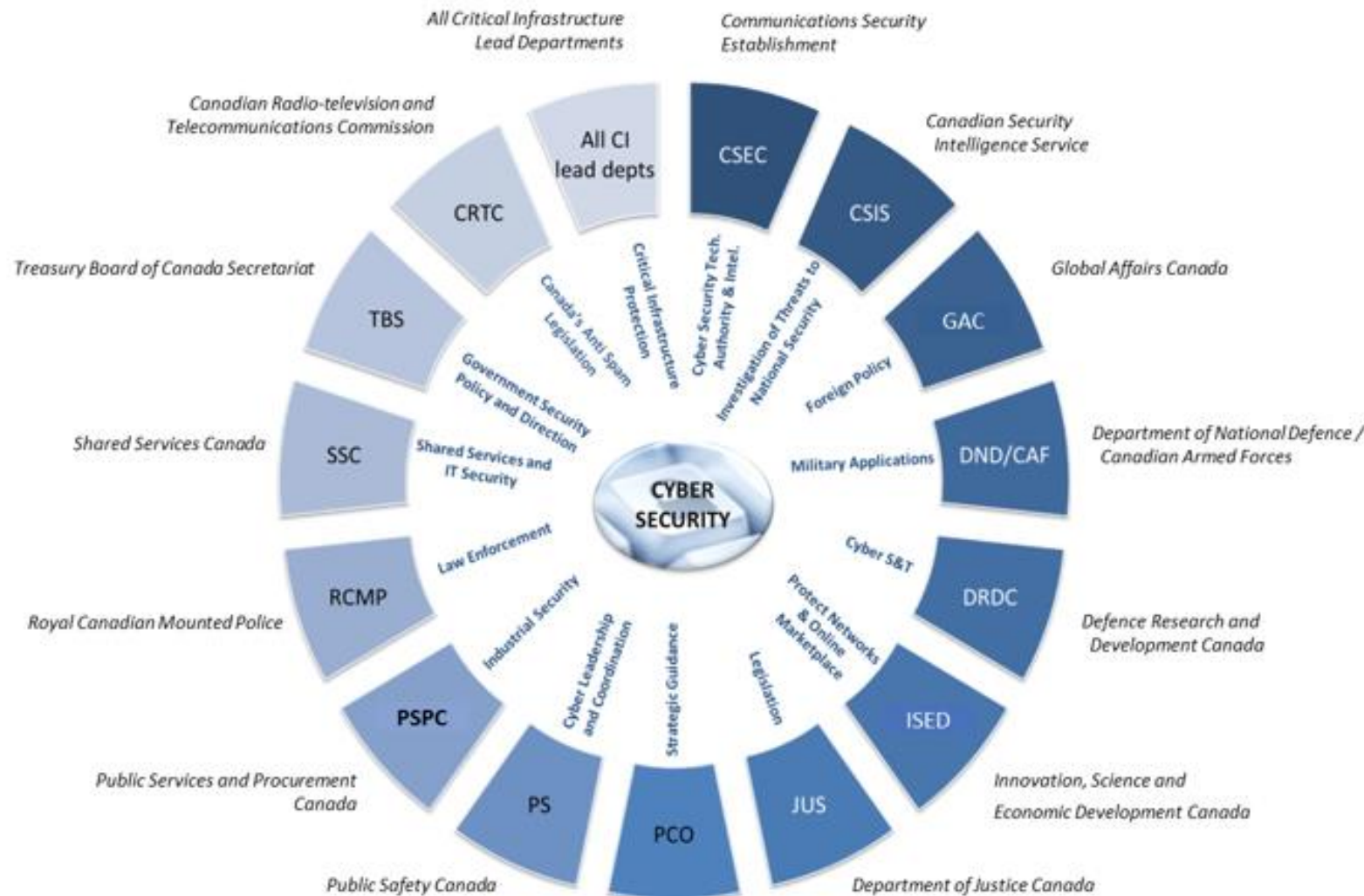


DEPARTMENTAL

All departments and agencies

Federal government departments remain responsible for their departmental cyber security

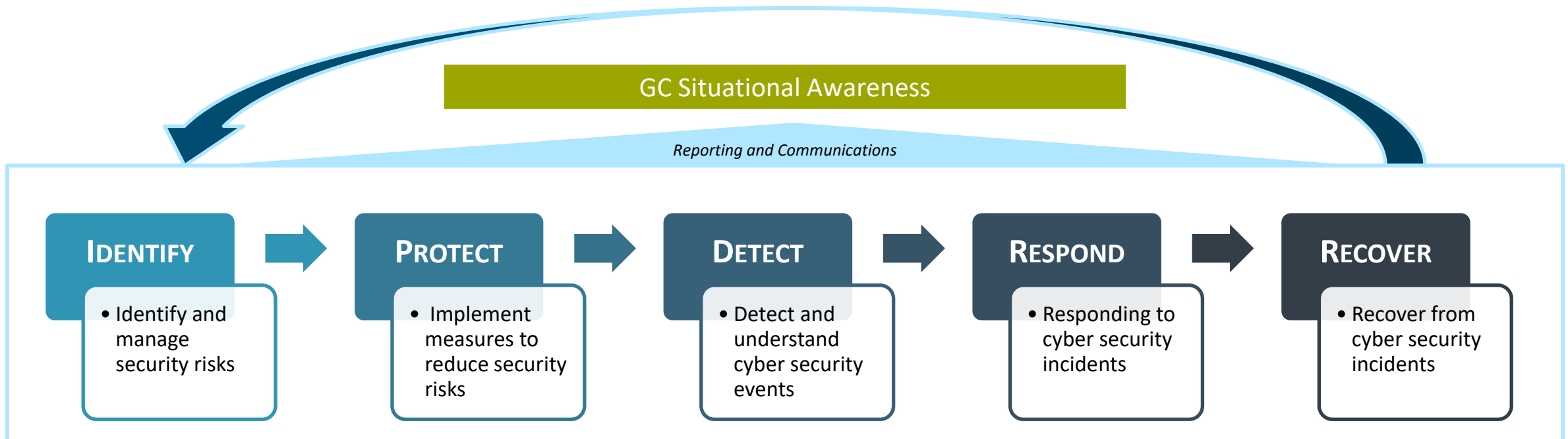
Cyber Security is a Shared Responsibility



TBS, the Canadian Centre for Cyber Security as an agency under CSE, and SSC combine to form the GC IT Security Tripartite, established to develop and maintain a coordinated and collaborative approach to enterprise IT Security

GC Cyber Security Management Process






Goal: Maintain visibility of enterprise cyberthreat and risk environment through continuous monitoring and ensuring the effective management of GC cyber security events

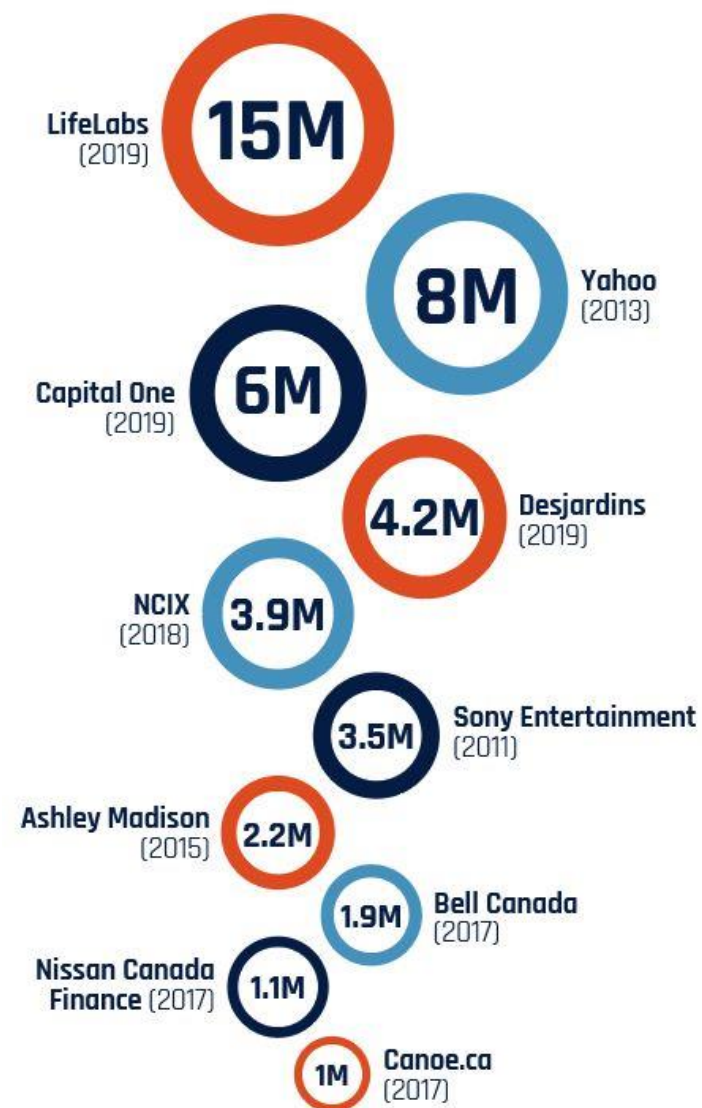


The background is a solid dark blue. Overlaid on the left side is a faint, circular, technical diagram. It features a central padlock shape, which is itself composed of several concentric, interlocking gear-like segments. The diagram is rendered in a lighter blue, almost white, color, giving it a subtle, watermark-like appearance. The overall aesthetic is technical and digital.

The Cyber Security Landscape

National Cyber Threat Assessment 2020: *An Evolving Threat Landscape*

- 1  More Connections Means More Physical Safety is At Risk
- 2  More Connections Means More of Economic Value is at Risk
- 3  More Collected Data Increases Privacy Risk
- 4  Threat Actors Are Becoming Better Organized and Equipped
- 5  The Internet is at a Crossroads



Today...



The “Castle and Moat” Approach to Securing the Enterprise



“Anywhere, Anytime Access”

User Needs



Security versus User Expectations



Users will find a way...



Continuous Security

Pillars for Securing #GCDigital



Policy



People

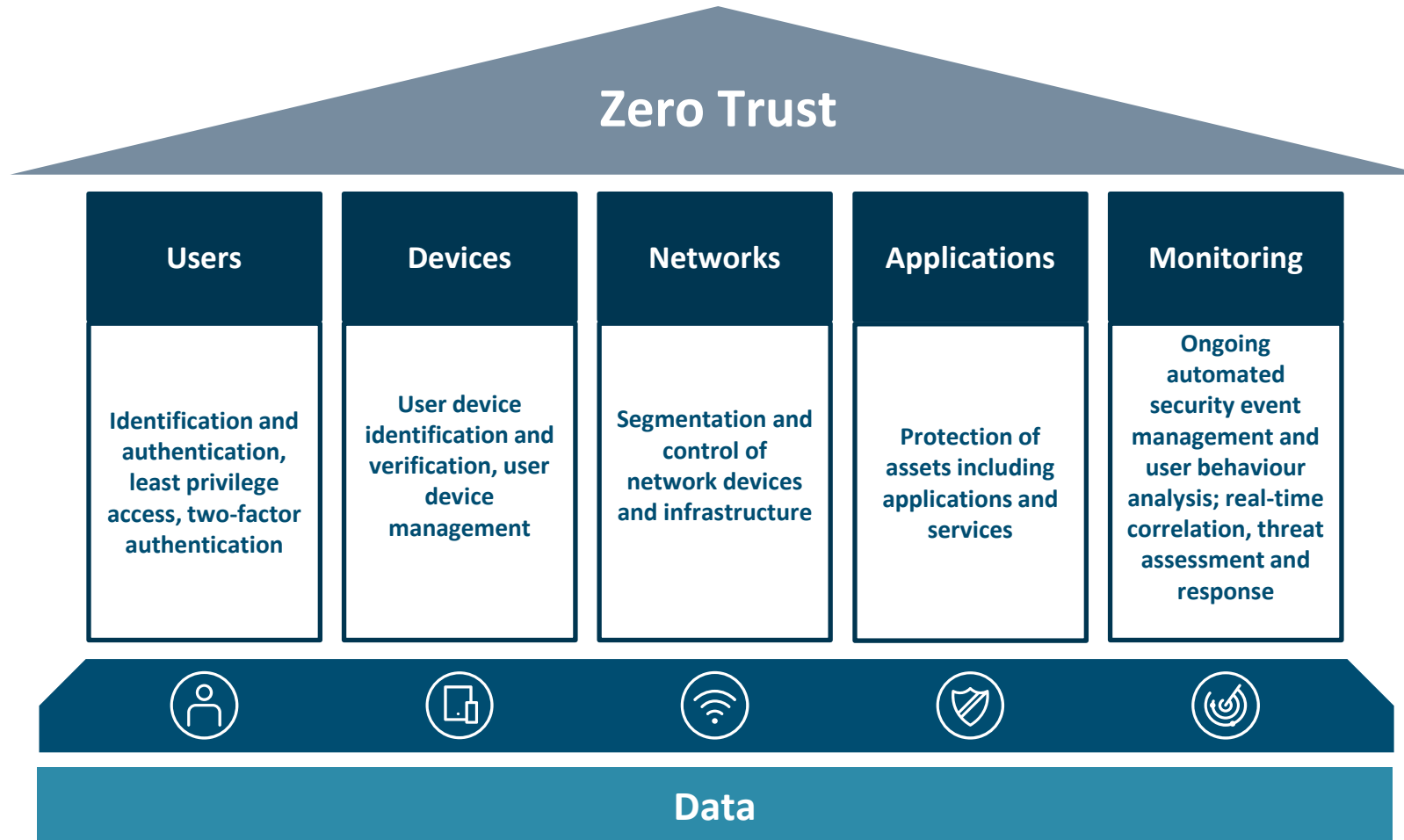


Process



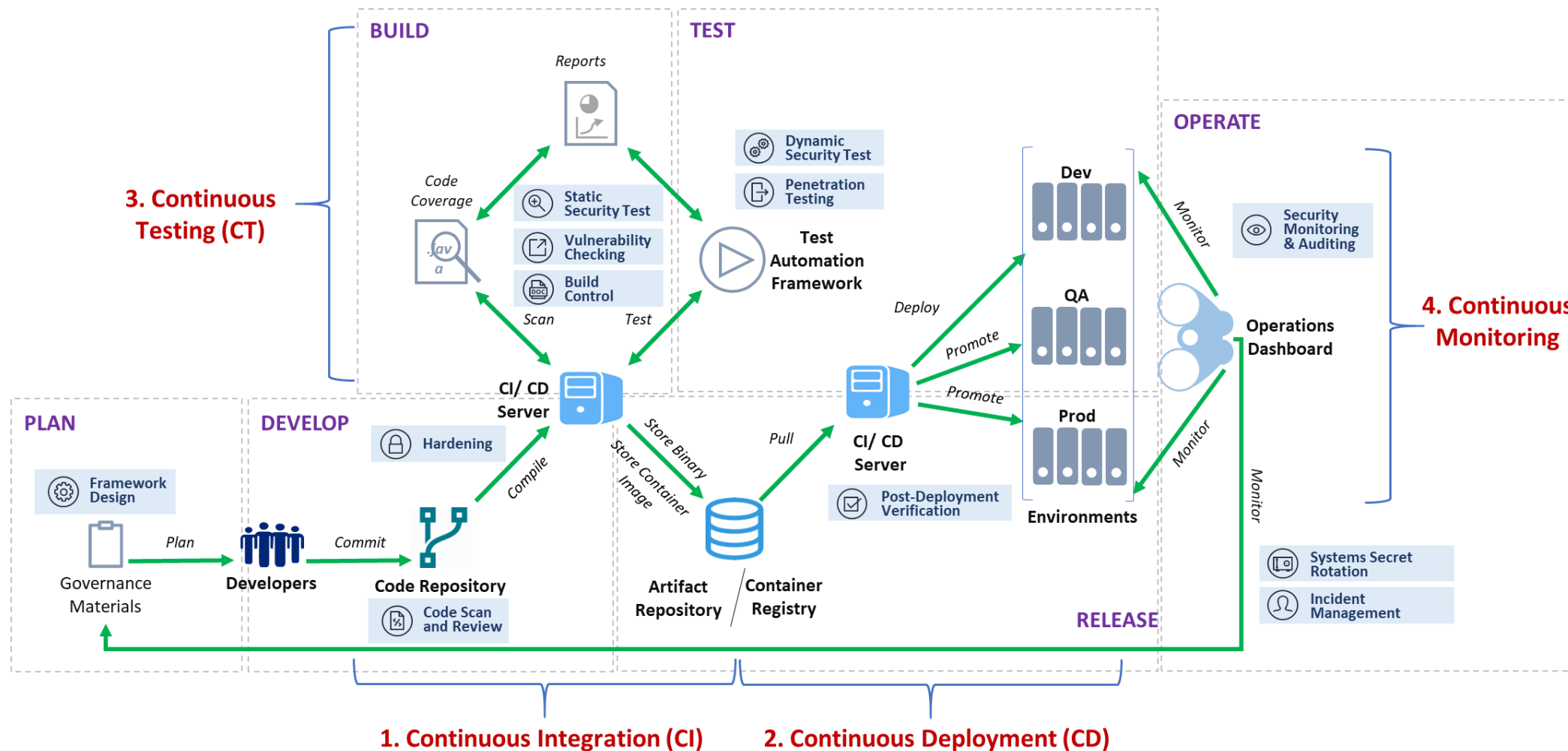
Technology

Evolving the security paradigm

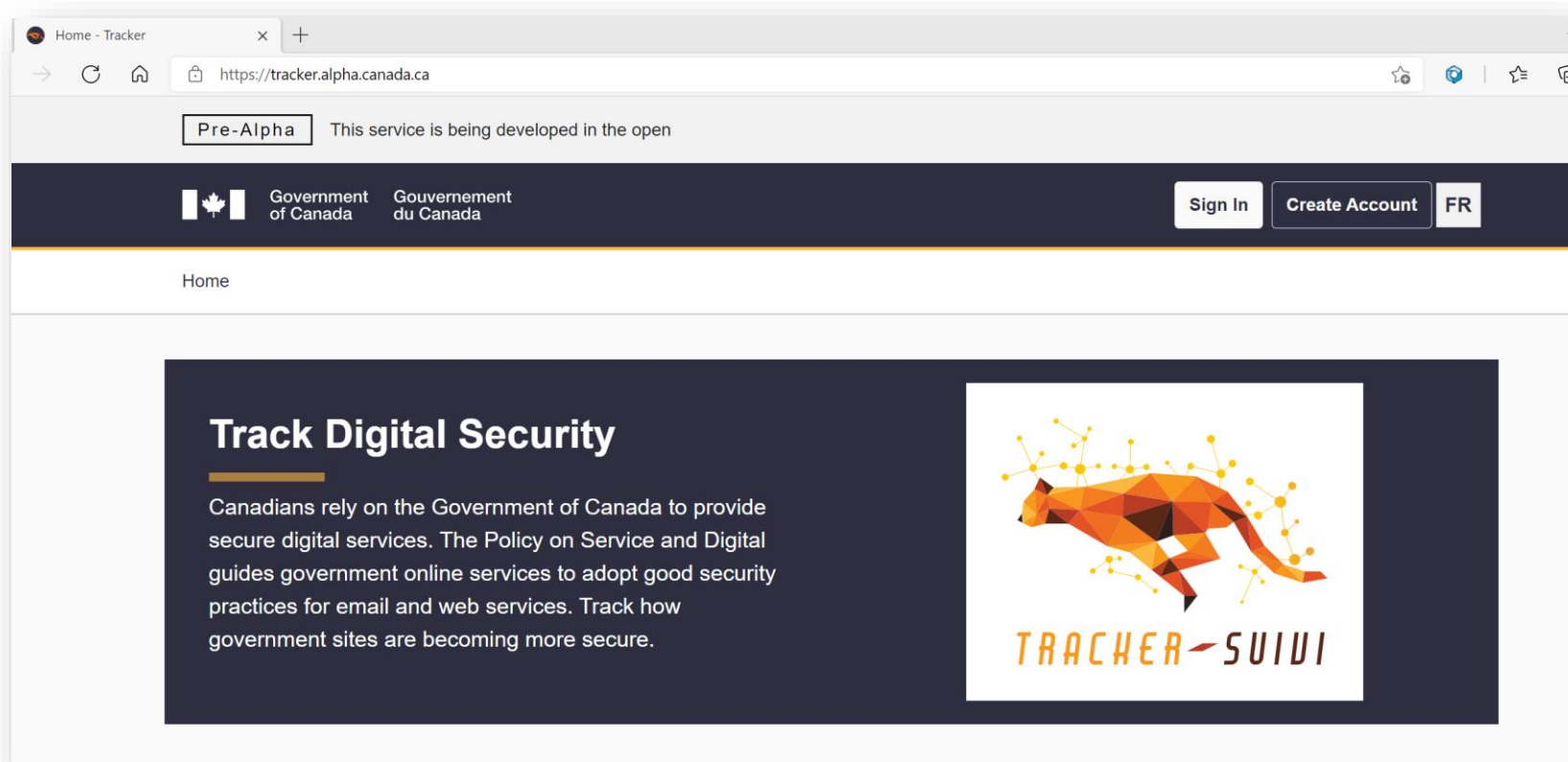




Build-in security. Shift left.



Case Study: Tracker 2.0



- ✓ Collaborative effort between TBS and CCCS
- ✓ Agile delivery
- ✓ Continuous integration/continuous deployment (CI/CD)
- ✓ Security by design
- ✓ Work in the open - <https://github.com/canada-ca/tracker>.
- ✓ Hosted in cloud
- ✓ Leverages open source software and tools

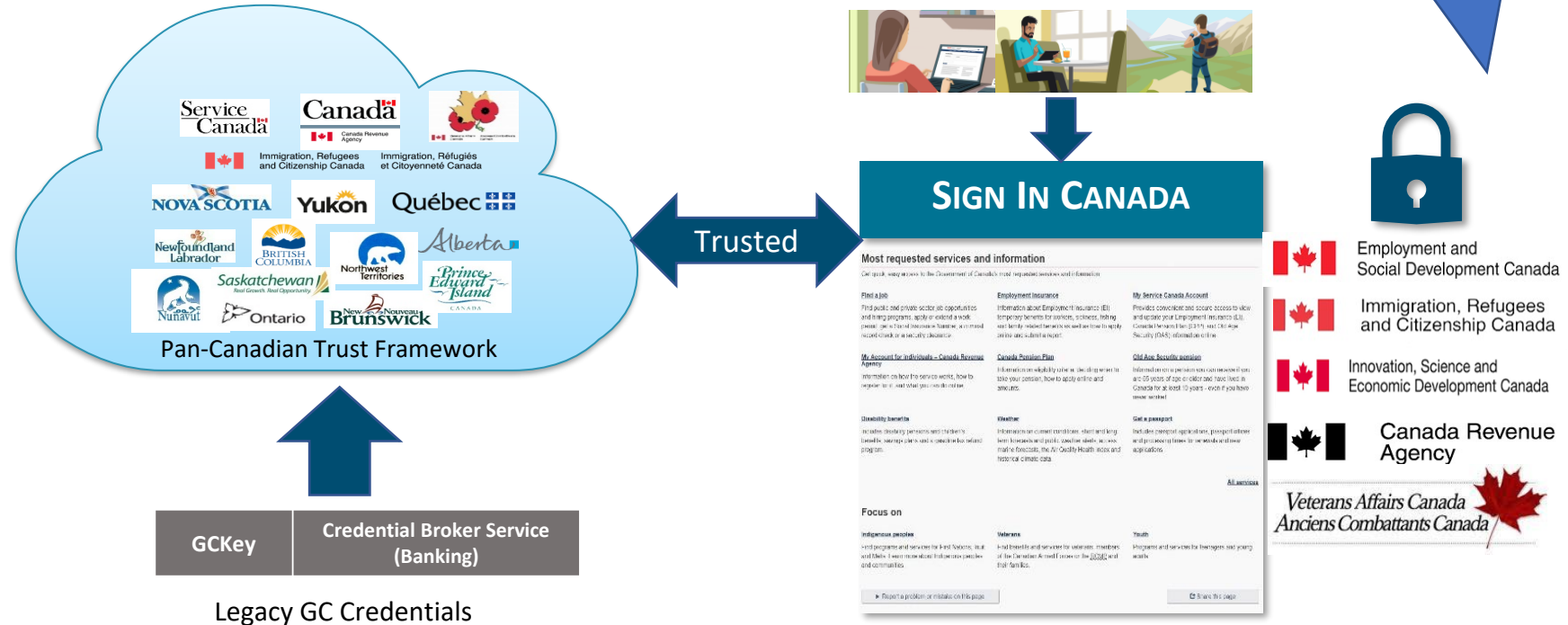


Digital Identity

Canada's Digital Identity Vision:

You only have to sign in once to deal with government

UNCLASSIFIED



The Government of Canada is enabling a digital identity ecosystem for the nation to:

- be leveraged by all GC departments and agencies, other jurisdictions in Canada (provinces, territories, municipalities) and Canadian partners (private sector & other countries)
- deliver services and issue digital identities to Canadians so they can access services seamlessly, anytime, anywhere and on any device.

Guiding Principles



Canadians at the
heart of the
service



One front door,
no wrong door



Secure and
Trusted



No one left
behind



Build one
ecosystem for
the benefit of all



Iterative,
adaptive, and
modular

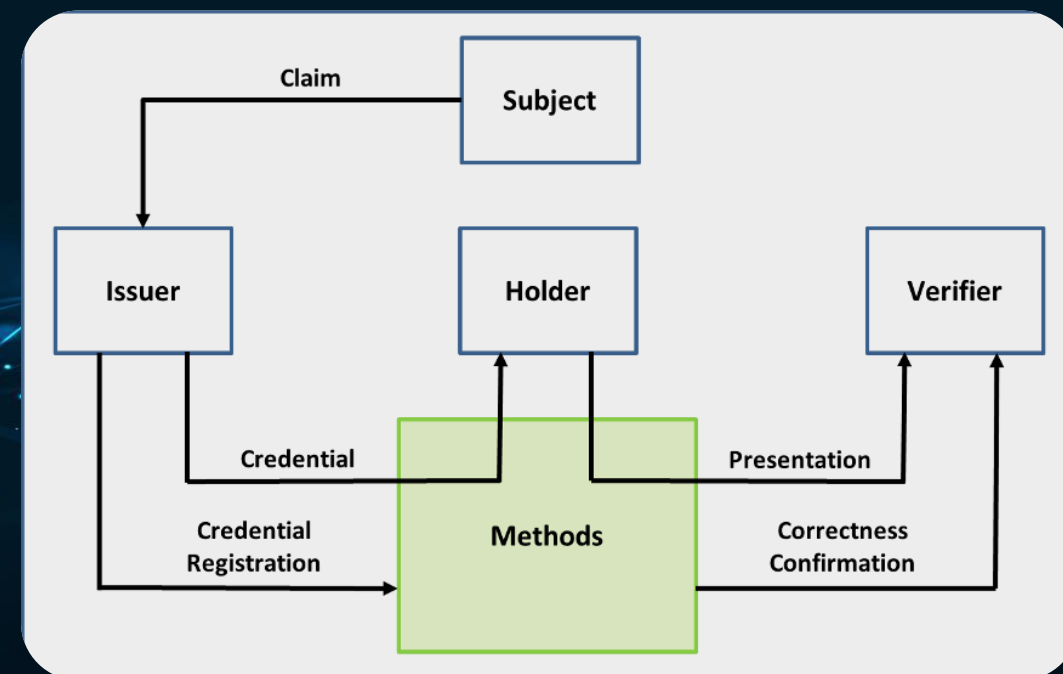


Respect
jurisdictional and
program
accountability

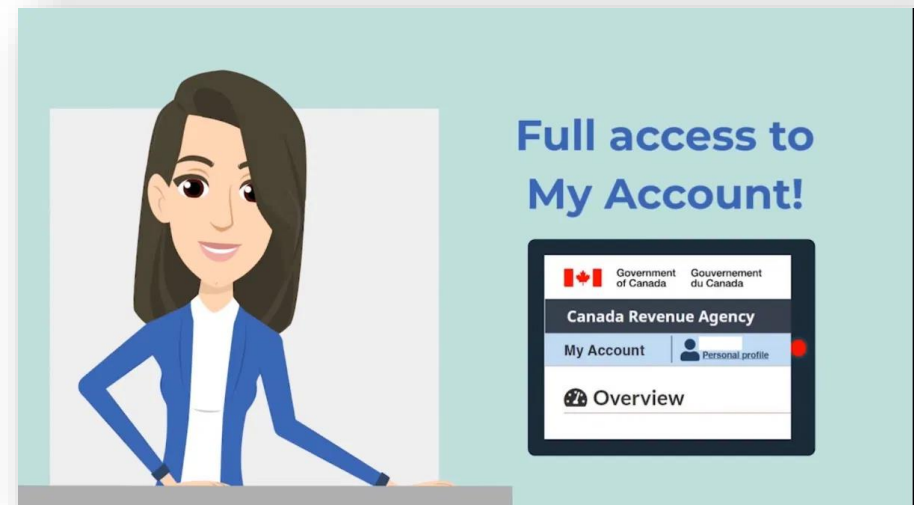
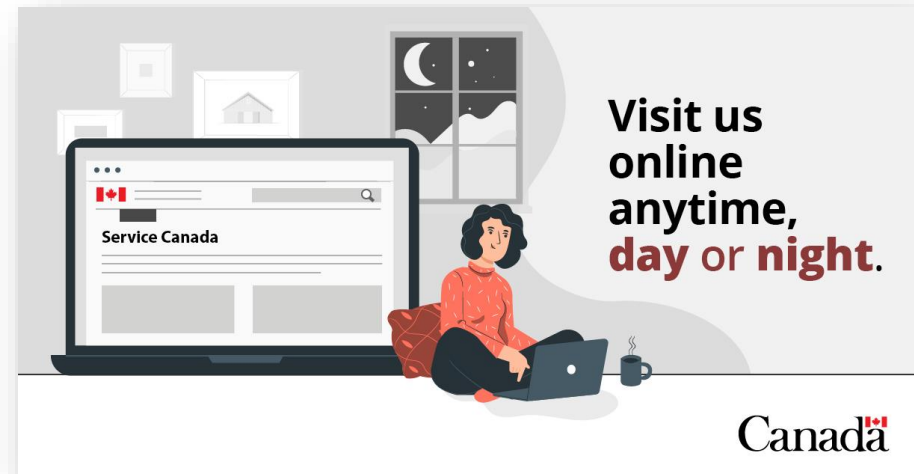
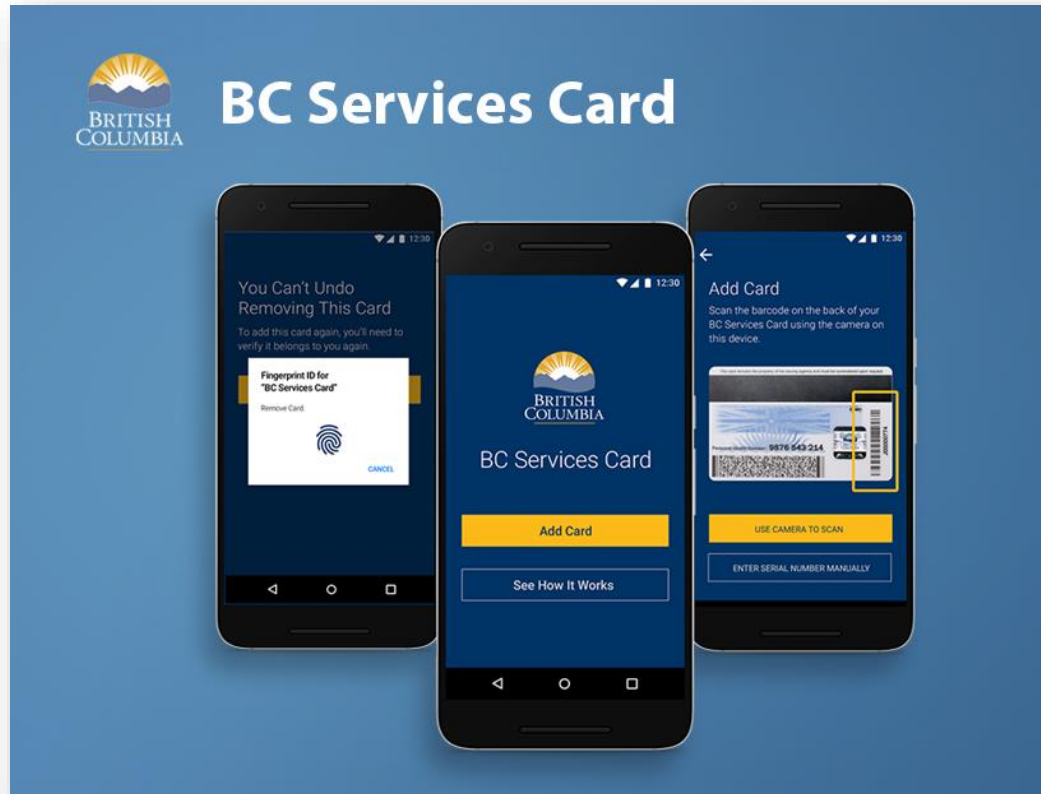
Establishing Trust

The Pan-Canadian Trust Framework (PCTF) is

- A model that consists of a **set of agreed-on** concepts, definitions, processes, conformance criteria, and an assessment approach to enable trust.
- A framework that **relates and applies** existing standards, policies, guidelines, and practices, and where such standards and policies do not exist, specifies additional criteria.
- Facilitates a **common approach** between the public sector and the private sector.



Case Study: Trusted Digital Identity Pilots



Key Takeaways



Security as a business enabler

Address security and privacy risks from the outset

Design services that are resilient

Apply a defence-in-depth, layered security approach

Collaborate & communicate



THANK YOU!

Contact us ZZTBSCYBERS@tbs-sct.gc.ca