Canada School of Public Service | École de la fonction publique du Canada

A Primer on Digital Technology

Canada

Overview

1. Introduction and trends
2. Basic components of technology
3. User access
4. Applications
5. Information and data
6. Servers and cloud
7. Networks
8. Security
9. Digital talent

Introduction

Advancements in digital technology continue to change the way **society operates** and **citizens' expectations for service delivery**

While digital technology is a **complex and technical** area, lending itself to specialists and experts, it is also **foundational to how one delivers** on their business priorities

Being familiar with the **basics of digital technology** can help you understand how they apply to your business and help respond to citizens' expectations

Keeping Pace with Change

Technology **evolves quickly** – and the rate of change is **accelerating**

Organizations

Organizations should build the capacity to experiment with emerging tech to **identify opportunities**

Systems

Systems and strategies should be designed to allow for **constant evolution**

People

Employees should be encouraged to regularly update **technology**, **skills and awareness**

Technology can be **optimized** by staying up-to-date and understanding key trends

Meta-trend 1: Low-cost Computing Power and Speed

A meta-trend is a foundational shift that enables, accelerates, or drives other changes and affordances.

Processing

Computers are now processing information of unprecedented **volume** and **complexity** unlocking new insights and usages

Storage

The **scale** of data storage that is commercially available has grown, enabling more digital service delivery options

Connectivity

Data can now be transmitted at a much higher **speed** than ever before, allowing real-time interactions and feedback

Enables:

Making copies of resources and **sharing information has become cheap or free**, changing the possibilities and value proposition of collaboration at scale

> e.g., **GC Notify** is a customized copy of an entire software project, but that powers communication to users for 440 government services

This orders-of-magnitude capability increase also enables the **resource-intensive data processing behind AI systems**

Meta-trend 2: Commoditization and Cloud

A meta-trend is a foundational shift that enables, accelerates, or drives other changes and affordances.

Commoditization

More and more parts of the IT value chain are **easily, repeatably accessible**

Cloud

Cloud services – **software (SaaS), platforms (PaaS), and infrastructure (IaaS)** – allow organizations to benefit from technologies on **demand**, in **flexible** ways

Microservices

Small, discrete **building blocks** of digital technology services which can be modular and scalable

Enables:

The modern software environment enables, and has revealed the need for, **user-centric test-and-iterate** approaches and continuous deployment – while requiring different governance for testing and releases

Services and businesses can add features and back-office services quickly and **according to need**, and changes can **be deployed and tested continuously.** E.g., **Shopify** allows any business to create a storefront and accept payments in minutes, at low cost

Services can **scale globally overnight**

Many technologies that once required extensive technical expertise are available through **mass-market, user-friendly interactions.** E.g., **ChatGPT** made sophisticated language models available to the world

GC Digital Standards

The Government of Canada has developed a series of **aspirational digital standards** to guide teams in designing digital services in a way that best serves Canadians

These standards are supported with a ***Playbook***, and are one piece of the overarching ***Government in a Digital Age*** agenda

The goal is to ensure the Government of Canada's digital services are **agile, open and user-centric**

See Annex B for Government of Canada Reference Material

Basic Components of Technology

Basic Components of Technology

User access

Application

Information and data

Server / Cloud

Network

A **technology stack** or **software stack** is a set of components that work together to support the execution of an application

The components may include an operating system, server, databases, one or multiple programming languages, content management systems, and the application layer (or front end) that users see

5 core building blocks are **user access, application, information/data, server/cloud,** and the **network**

Each layer requires skills, decisions, and infrastructure, and enables different affordances for how the GC operates and delivers, from policy to delivery

User Access: For Employees

"Access" requires both a device and a user profile to log in

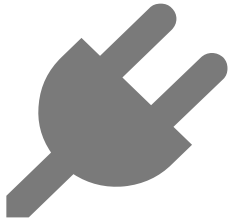
Employees access data and applications on **their device** based on credentials assigned to **their profile**

SSC **procures devices** for departments, based on their **business needs**

Departments **configure user profiles** and provide **ongoing support**

User Access: For Employees

Device needs vary by user – ensure you have the flexibility to meet the needs of all your employees



COMPUTING POWER

Some users may require **more computing power** (e.g. data scientists)

MOBILITY

Devices should be **small** and must be able to **connect remotely** for employees

ACCESSIBILITY

Devices need to **meet the needs of all employees**, and some employees will require assistive and adaptive technologies

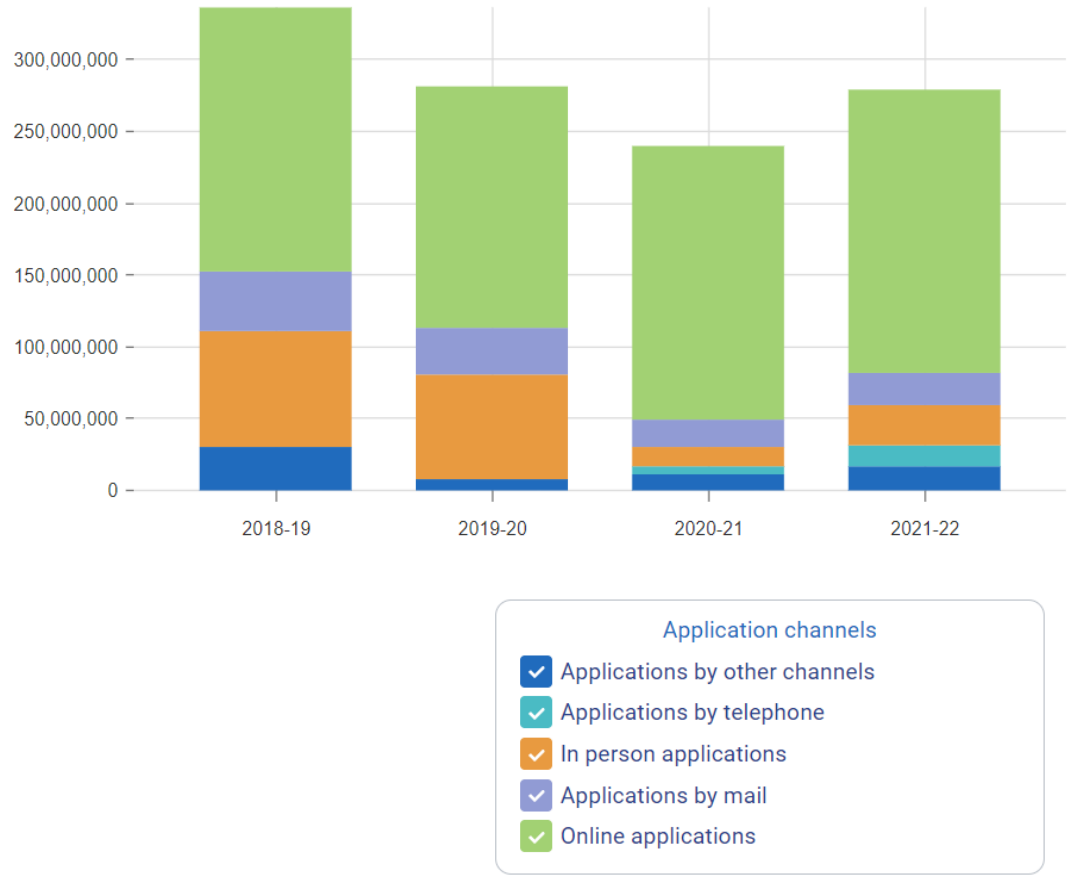
Older devices may have **performance** issues when running modern applications and **may be hard or impossible** to keep updated for security.

User Access: Accessing GC Services

In **2021-22, 78** departments and Government of Canada agencies accepted **279,470,479** applications via **1,848** services. **70% were completed online**, but as of 2021-2022, 80% of government services are not available end-to-end online

GC services and content must be designed for **accessibility, inclusivity, readability,** in some cases **specialized audiences,** and different **devices and screen sizes**

Many GC services are still difficult to navigate, and test-and-iterate approaches often raise task completion rates from 50-60% to 80-90%



Applications

"Applications" are discrete pieces of software* designed to perform specific tasks

Employees use **applications** installed on **devices** and **servers** to accomplish their work

Traditionally, organizations bought, configured, and operated **their own applications**

This approach can have disadvantages: duplication of effort, increased cost, data silos

Increasingly organizations are contracting **third parties** to do this work (Software as a Service, or SaaS)

Examples

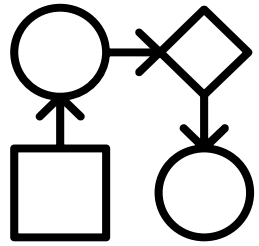
- Microsoft Teams: videoconferencing and collaboration software
- Google Search: a common web-based application
- SAP: one of the GC's financial and materiel management systems (built by the private sector)

*See ANNEX E: Glossary of Terms for definition

** Increasingly, private companies use open-source technology and standards

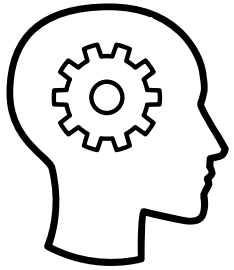
Applications

It is essential to understand how to get the most out of each application



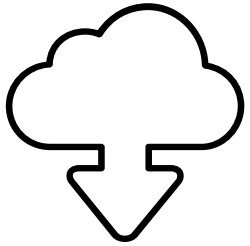
Process > Application

Many applications replace paper-based processes – but digitizing dysfunctional business processes will not make them better and simply amplify the dysfunction



UX
(User Experience)

Applications are user-facing, and should be designed with users; meeting functional requirements does not mean that people can or will use an application



Updates

Applications should be updated regularly (can be daily) to prevent security vulnerabilities, to fix problems “bugs,” and to add functionality

Data

Public sector organizations **generate, hold, and use** a vast and diverse array of data for research, science, program administration, evaluation, accountability/transparency, operations, and more.

Source	Purpose	Characteristic
• **Administrative activities:** birth records, employment records • **Research**: species population, water quality • **Written documents**: briefing notes, laws • **Maps / geospatial data**: climate models, flood plain maps	• **Regulation, security and enforcement** • **Services delivery** • **Operations** • **Research, policy development and programs**	• **Quantitative** data is data that can be counted or measured in numerical values • **Qualitative** data cannot be counted, measured or easily expressed using numbers • **Structured** data consists of clearly defined data types whose patterns makes them easily searchable • **Unstructured** data is not organized into a data model (e.g., audio files or the content of emails)

Data, Information, and Knowledge

Data, on its own, is an asset – but must be curated and analyzed to create information and knowledge, best driven by clear business questions.

10 01 10 01
01 10 01 10
10 01 10 01
01 10 01 10
10 01 10 01

Data

Raw facts and figures, lacking interpretation or analysis

Information

The interpretation of data

Knowledge

Information combined with subject matter expertise to create meaningful insights

Data, Information, and Knowledge

The fields of data and AI are evolving rapidly, along with the GC's needs in these spaces

1. The amount of data generated is growing exponentially

- From internet use, computing-enabled research methods, and networks of everyday objects and infrastructure connected to the internet

2. Analytic approaches and computing power are advancing

- Increasing ability to analyze big data (massive datasets) to find patterns and make predictions

3. Data skills and expertise remains a challenge

- Without in-depth knowledge of how to analyze and interpret data, or investments in scaling infrastructure, organizations are limited in their ability to make full use of data

AI technology is advancing rapidly, enabling and requiring new techniques, tools, and skills

- Automation
- Data mining
- Decision/process support
- Generative AI

Interoperable and linked data

While the GC holds substantial data assets, it's often siloed by its structure

Designing for interoperability can increase the value, accuracy, and reusability of data – and improve program and policy decisions

There are a range of models, standards, practices, and technologies to support the integration of different data and datasets: rules for structuring and labelling datasets (metadata standards), linked data ecosystems, and more

Common data fields and requirements allow administrative fluidity – e.g., HR transfers – between GC organizations without substantial manual entry or data conversion

At the program and policy level, approaches like the Social Data Linkage Environment at Statistics Canada connect existing socioeconomic data and allow higher quality analysis without additional data collection

Data can be shared within GC organizations, between GC organizations, or with external partners and stakeholders – but there are real and perceived barriers related to governance

The 5-Star Data Model used by open.canada.ca (the GC's open data portal):

★	Make your data available (whatever format) and re-useable
★★	Make it available as structured data (e.g., Excel instead of image scan of a table)
★★★	Use non-proprietary formats (e.g., CSV instead of Excel)
★★★★	Use standard resource locators, so that people can point at your data
★★★★★	Link your data to other data to provide context

AI, data, and algorithms

Artificial intelligence (AI)

An **AI system** is a machine-based system that infers how to generate outputs such as predictions, content, recommendations, or decisions from the input it receives

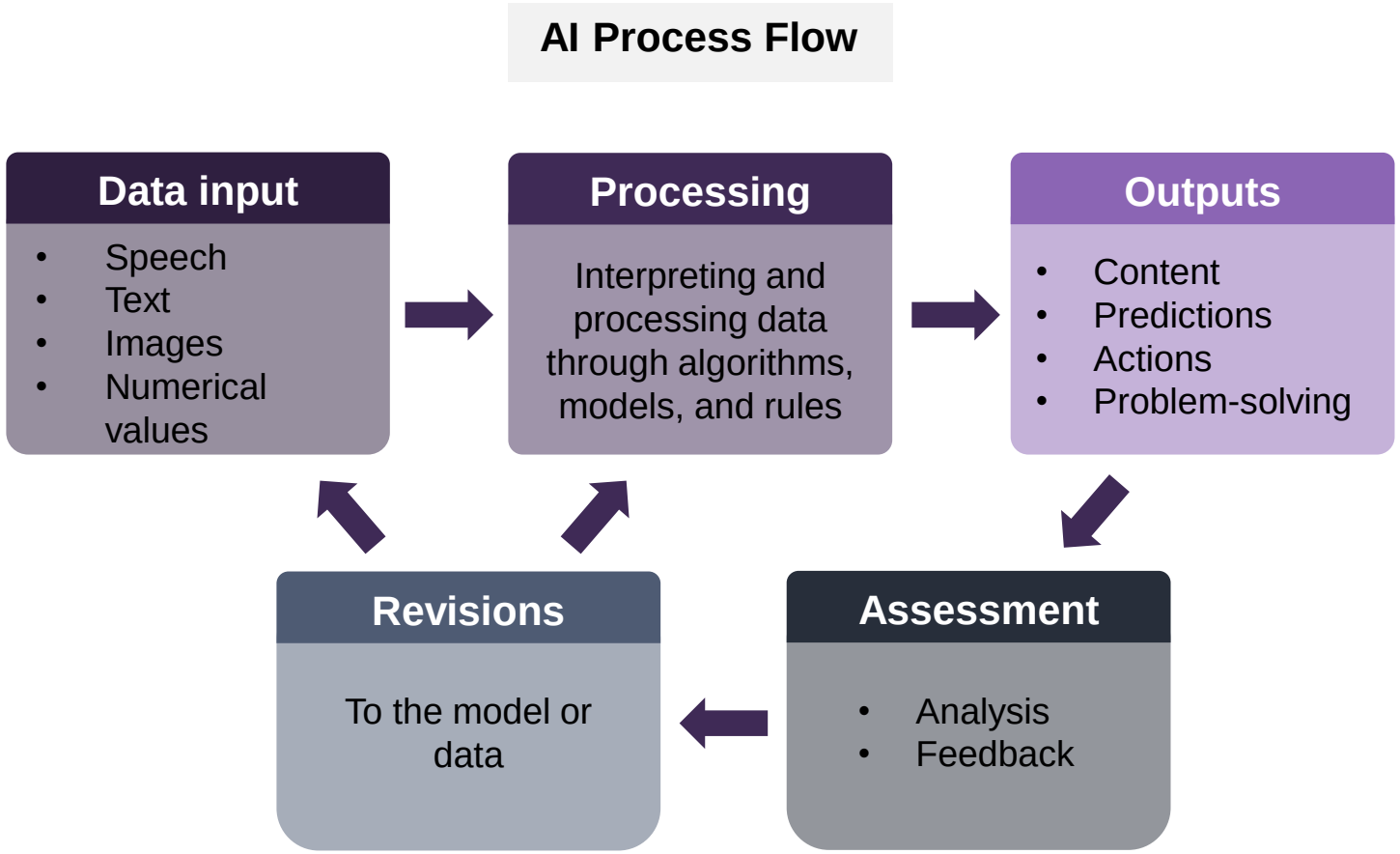
AI is also a **category of technologies**; a common explainer is “technology that performs tasks that would ordinarily require biological brainpower to accomplish, such as making sense of spoken language, learning behaviours, or solving problems”[1]

Data

AI systems get their value from processing massive amounts of data – and are generally required to process that data in the first place

Algorithm

An algorithm is a set of rules or instructions a machine (and especially a computer) follows to achieve a particular goal



Servers

Servers store data and information and provide computing power to run applications – they can be managed through in-house data centres* or through third-party Cloud solutions

GC owned and operated		Privately owned and operated
1 Legacy Data Centres*	**2 Enterprise Data Centres***	**3 Cloud**

• Older facilities that serve one department, or a cluster of departments
• Aging infrastructure and expiring leases are risks to reliable access
	• New, state-of-the-art facilities to serve the entire federal government
	• GC retains responsibility for maintenance and evolution of the technology
	• Lots of capacity available
		• Public and private solutions run by a third party, accessed over the internet
		• Servers are not always in Canada**
		  • Unclassified and Protected A – no policy restrictions
		  • Protected B, Protected C and Classified – Canada is the preferred option

Data Centre: A large group of networked computer servers typically used for the storage, processing, or distribution of large amounts of data.

****Data Residency policy*** can be found in section 4.4 of the Guideline on Serivce and Digital. Canada is the preferred option but departmental CIOs can make a risk-based decision related to data residency

Servers: Cloud

Increasingly, organizations are becoming consumers of services that provide storage, compute, and business solutions from third-party commercial cloud providers

Cloud is like a utility service (e.g., hydro) and reduces the need to internally own, operate and renew technology components.
Benefits include:

- **Economies of Scale:** No up-front investment required; cloud providers ensure storage technology is up to date
- **Elasticity:** More space can be purchased instantly; reductions in storage space result in lower costs
- **Resilience:** Data is distributed across multiple locations, ensuring redundancy if one of them fails

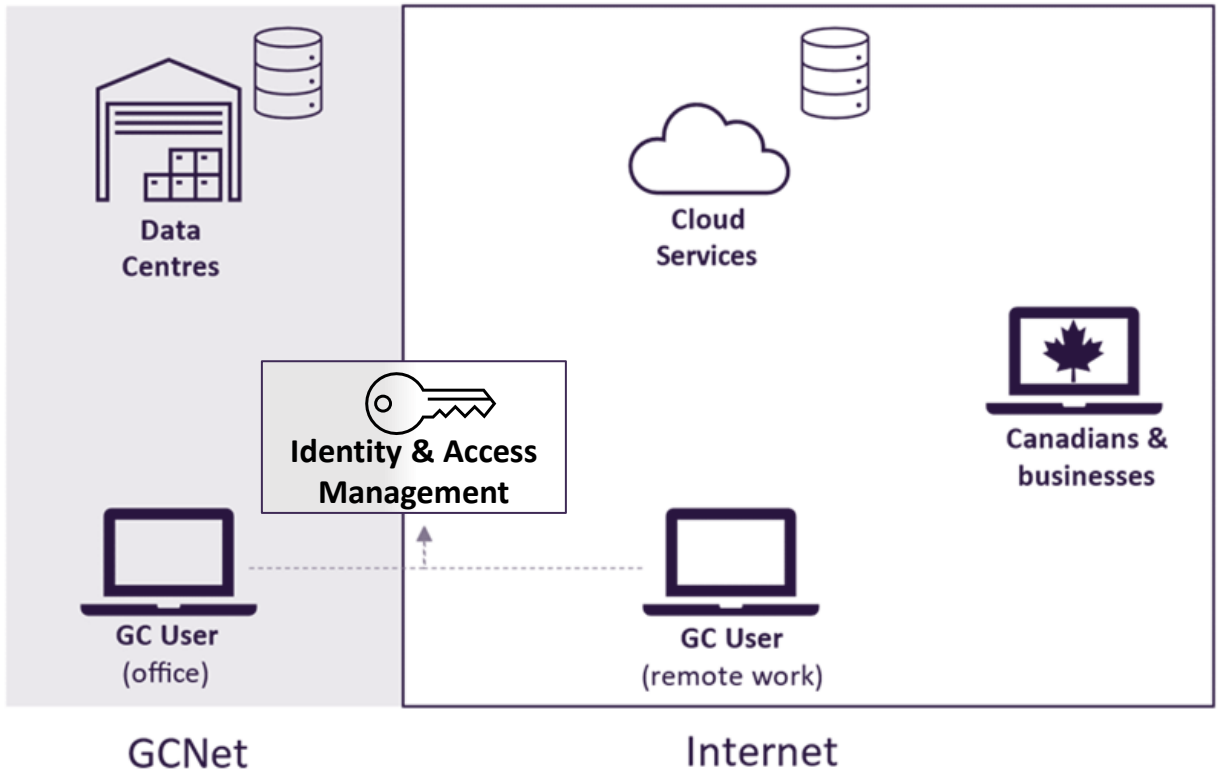
Tech is increasingly outsourced, shifting to **'as-a-service' models**:

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

See Annex C for more details

Networks

"Network" refers to any wired or wireless **connection** between two or more computers



Commonly accessed networks

GCNet: connects GC devices to data centres and to the Internet

GC Secret Infrastructure: connects various classified information networks in the GC. It is a segregated from all other networks

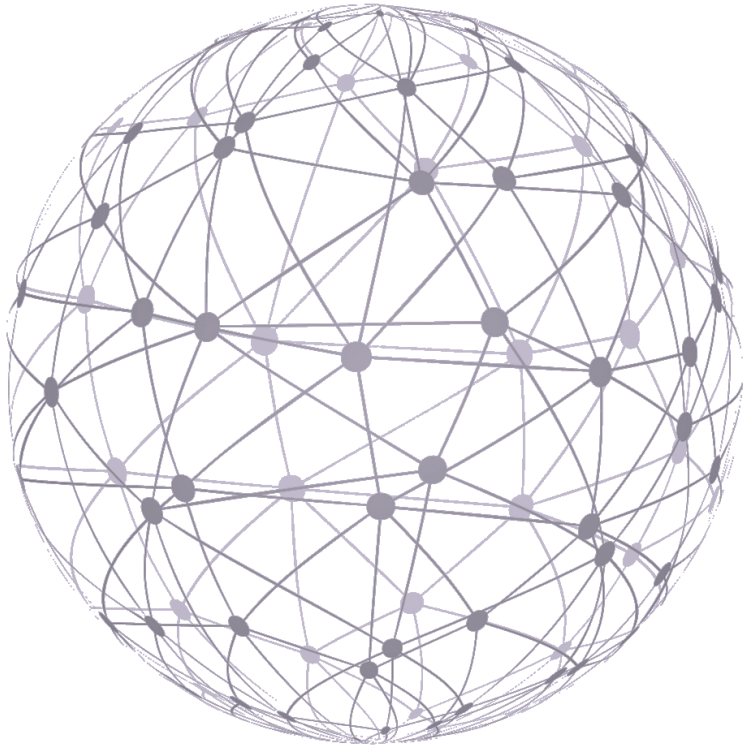
Virtual Private Networks (VPN): a private network that operates across a public one, enabling remote access (e.g. from home) to the GC's internal network.

Wi-Fi: on-site wireless Internet connectivity for employees or guests

Firewall: monitors incoming and outgoing network activity against a set of security rules

Networks

Your networks need to be configured to enable **reliable, secure access when and where** your employees need it.



Allow **secure remote access** with reliable VPNs required to allow employees to work remotely without losing productivity

Enable **real-time collaboration** with Microsoft 365 tools like Teams (in particular for videoconferencing) that require adequate bandwidth to perform correctly

Promote **flexible workspaces** with consistent and fast Wi-Fi required in modern working environments

Security

Security refers to **assurances** that government information and assets are ***protected*** against threats to their confidentiality, integrity, availability, or value

Security controls are in place to protect **all elements** of government systems from threats

Our IT systems hold information of great **business value** (e.g., national defence information), and **personal value** (e.g., Canadians' tax filing information)

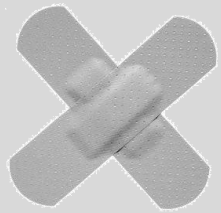
Government operations rely on the **fast and efficient flow of information** – security breaches can be very expensive and slow to resolve, damaging our ability to do business and Canadians' trust in government

Security: Best Practices

The following **best practices** can address IT vulnerabilities. These vulnerabilities may include **accidental** or **malicious** threats from **inside** or **outside** your organization

External threats are constantly evolving; requiring dynamic defences

Ensure capacity and expertise for ongoing cyber security protections



Update software continuously to protect against vulnerabilities

Safeguard sensitive information (both cyber and physical security)

Internal threats also pose serious risks, and require dedicated attention

Provide appropriate security classifications for employees (personnel security)

Provide training; human error is a key source of security vulnerabilities

Carefully manage access to administrative privileges

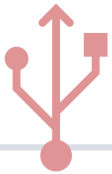
Digital Talent

Digital Talent

The Government of Canada aims to **attract tech talent** with certain digital mindsets, skills, and approaches

Top talent with the **mindsets** to design products with the **user at the centre**, using **creative approaches** to solve problems

Skills that range **from computer science,** to **STEM**, **design**, **DevOps** and more – partnered together

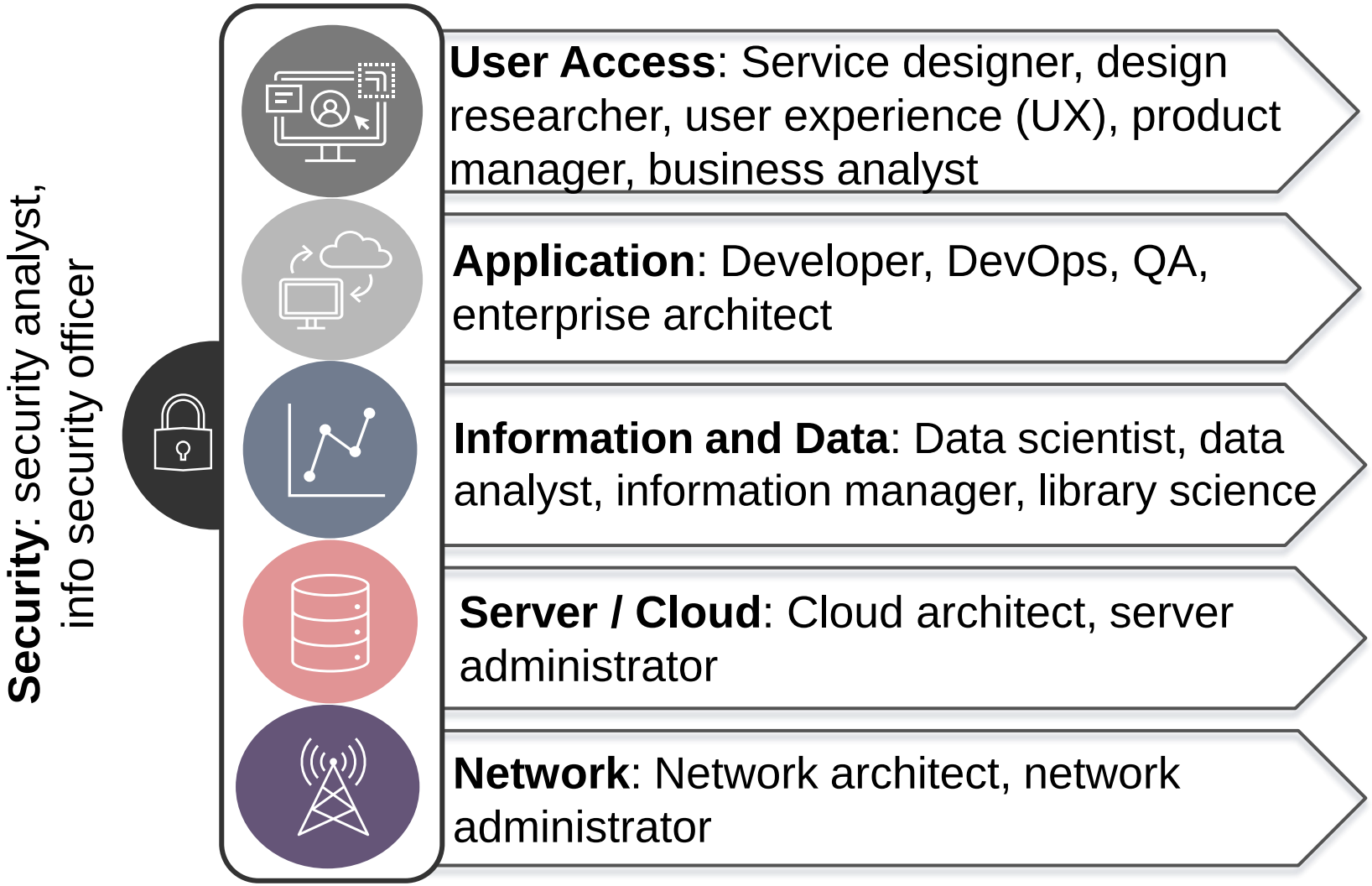


Approaches such as **open-source**, and **agile** methods

(**Agile:** build prototypes quickly and iterate based on user feedback)

Furthermore, **all government employees** need to be **digital** and **data literate** to encourage and enhance productivity, collaboration, data and information management, cyber security, and more

Examples of Tech Professionals



Building and Supporting Tech Teams

Building cross-functional technical teams can be challenging – some things to keep in mind:

Your team needs to **keep up** with the latest technology trends and tools, understanding how these can be applied to your business

This requires regular investments in **learning** and **development**

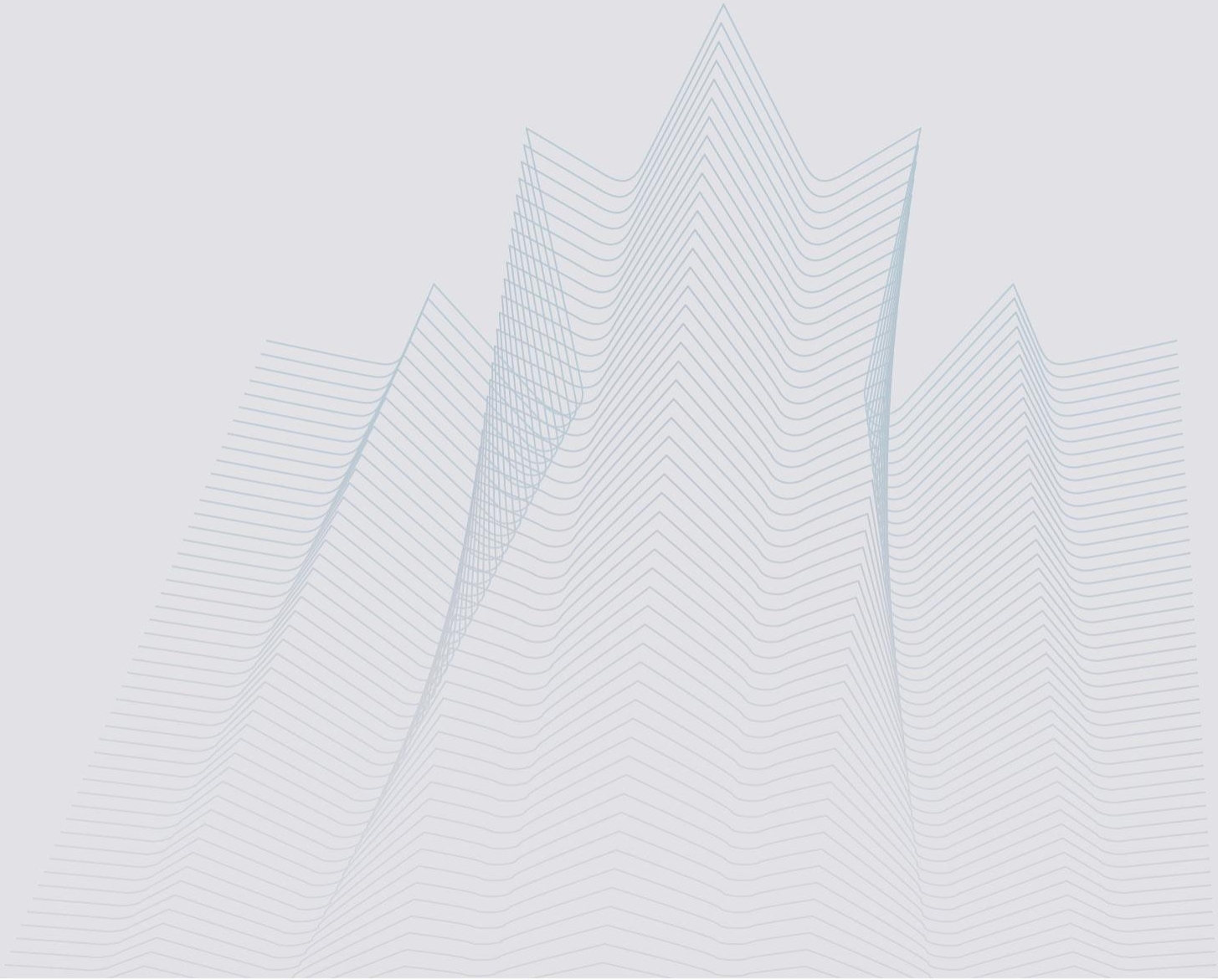
At the same time – until they can be retired, you need to **maintain** the know how required for **legacy systems**

Remember that **competition** for top tech talent with the private sector is intense

Public sector organizations have to be creative to attract talent
(e.g., remote working or short-term contracts)

You should understand the **background** (i.e., skills, training, and experience) of your tech team, as it may influence their **preferred solutions**

Annexes



Annex A: Roles & Responsibilities

Your department is only responsible for some components of the tech system…

User Devices (includes security)	
SSC & PSPC	*Procurement*
Departments[1]	*Configuration, security, etc.*
Data (includes security)	
Departments	*All Elements*
Applications (includes procurement, maintenance, security, and use)	
SSC	*Enterprise-wide Applications*
Departments	*Departmental Applications*
Servers (includes procurement, maintenance security and use)	
SSC[2]	*Data Centres and Computing*
Departments	*Cloud (with brokering from SSC)*
Networks (includes procurement, maintenance, and security)	
SSC	*All Elements*
Security *(responsibility is distributed across departments and agencies[3])*	

…but there are areas of **shared responsibility** where collaboration is required

Applications (department responsibility) need to be moved to **modern data centres or Cloud** (SSC responsibility)

This requires good communication, collaboration, and discipline to prioritize and execute

[1] "Departments" includes departments and agencies that are considered partners with SSC
[2] With the exception of Small Departments and Agencies that were included as SSC clients in OiC 2015-1071, who have the option of continuing to maintain their own legacy data centres and systems
[3] Section 5 of the Policy on Government Security outlines responsibilities for 10 lead security agencies

Annex B: Government of Canada Reference Material

Policy and direction:

1. **Policy on Service and Digital:** Authority for the Chief Information Officer of Canada to support workforce capacity and capability of the digital functional community: increasing digital skills is one of many ways to increase capacity.

2. **Canada's Digital Ambition:** A digital government-wide goal; all of which rely on some aspect of digital skills: technology and operations; data-enabled services and program; action-ready policy; and funding, talent and culture.

3. **GC Digital Standards:** The digital skills and associated learning and development opportunities for all public servants, executives, and managers must be aligned and build off the GC Digital Standards.

4. **2023–2026 Data Strategy for the Federal Public Service:** The Strategy outlines the current policy landscape that relates to data, describes a long-term strategic vision, and identifies actions over the next three years that will move the public service closer to that goal.

5. **Responsible use of Artificial Intelligence (TBS)**

6. **Protecting Information when using applications (Cyber Centre)**

Learning:

Courses

- How to be Digital in the Canadian Public Service (DDN201)
- A Self-Directed Guide to Understanding Data (DDN303)
- Introduction to Human-Centred Design (DDN207)
- Introduction to Agile in the Public Service (DDN208)
- Introduction to Product Management in the Public Service (DDN236)
- Discover Cyber Security (DDN235)
- Discover Artificial Intelligence (DDN210)
- Discover GC Cloud (DDN104)
- Introduction to IT Security Management (DDN106)
- IT Security Fundamentals for IT Practitioners (DDN107)

Microlearning

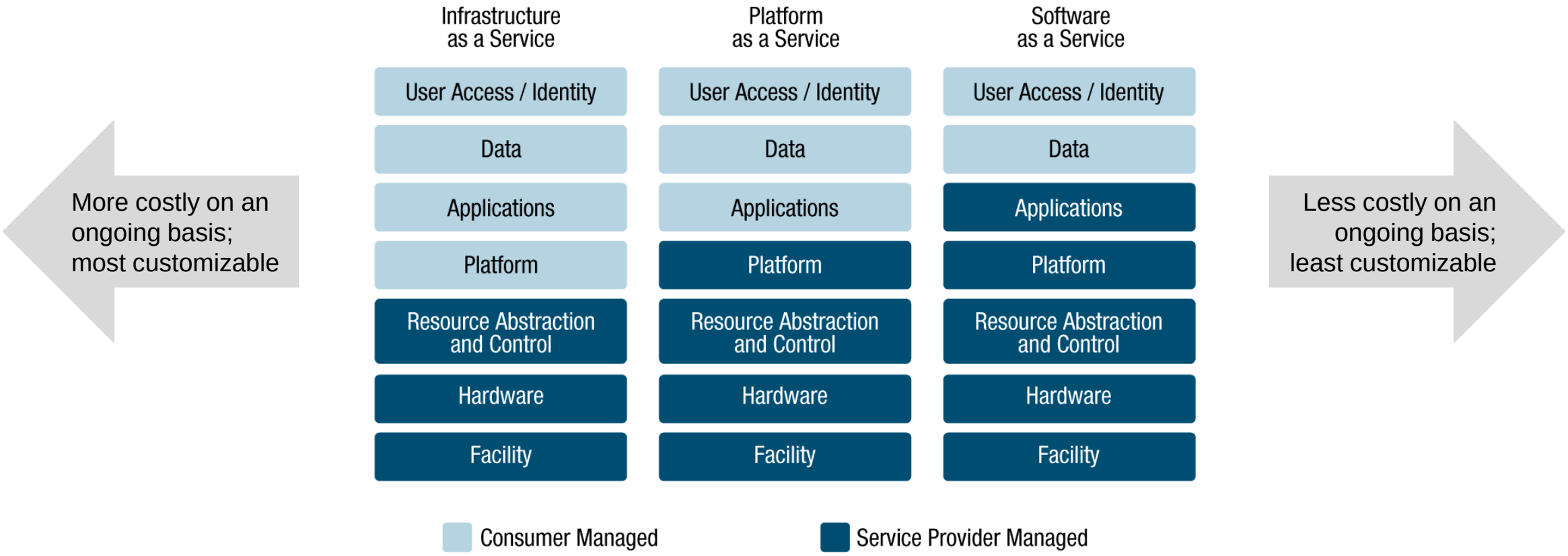
- How to be Digital in the Government of Canada (video)
- CSPS Digital Academy microlearning articles

Terminology

- The Tech Terms Computer Dictionary
- The EGN Digital Dictionary for Executives and (other) Tech-novices
- 99 Terms You Need To Know When You're New To Tech

Annex C: Cloud Service Models

Cloud is predicated on the idea of outsourcing various parts of your ‘technology stack” – there are many models of cloud, but three common ones include:



Annex D: Information and Data Responsibilities

The public sector has responsibilities associated with its data:

Stewardship	Openness	Privacy	Security	Transparency	Integration	Quality
Use business needs to determine data needs and associated processes, application, and IT	Maximize the release of data consistent with privacy, and security rules	Protect personal data in accordance with applicable legislation	Ensure personnel screening, and physical and cyber security safeguards are commensurate with relative risk associated with the data	Document how data is used in operations and decision making	Make data and technology reliable and interoperable	ensure data is consistent, complete, timely and accurate

Annex E: Glossary of Terms

Table of Glossary of Terms	
Agile	A development approach that delivers software in increments by following the principles of the Manifesto for Agile Software Development**.**
Artificial Intelligence	An AI system is a machine-based system that infers how to generate outputs such as predictions, content, recommendations, or decisions from the input it receives.
Bandwidth	The capacity for data transfer of an electronic communications system. Commonly expressed in bits per second (bps), megabits per second (Mbps), or gigabits per second (Gbps).
Computing Power	How fast a machine can perform an operation.
Hardware	encompasses all of the physical parts of a computer system—monitors, hard drives, servers etc. Software and hardware exist in unison to make computers work, each depending on the other to carry out our instructions.
Information Management	A discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal or long-term preservation.
Information Technology	Any equipment or system that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of information or data. It includes all matters concerned with the design, development, installation, and implementation of information systems and applications to meet business requirements.
IT Workload	The amount of processing that a computer is doing at a point in time.
Patch	A set of changes to a computer program or its supporting data designed to update, fix, or improve it.
Processing	Activity of a computer executing a program, or lines of code
Software	the way instructions are given to computers. Software programmers write in coding languages like ‘Python’ and ‘Javascript’, which are ultimately translated into binary code (machine language) instructing the computer to turn off and on various electrical circuits and perform actions.