



# Chief Information Officer Branch, Treasury Board of Canada Secretariat

**Donald Lemieux**

**David Schwartz**

**Stephen Walker**

**Chuck Henry**



# Agenda

- Access to Information & Privacy
- Security
- Information Management
- Information Technology

10 minutes each – it will be more exciting than you imagine!





# Agenda

- **Access to Information & Privacy**
- Security
- Information Management
- Information Technology

# What's the common thread?

*Information is the cornerstone of a democratic, effective, and accountable government...*

## Access to Information & Privacy

Citizens must have access to government information and decisions to participate in the democratic process

Protecting privacy implies safeguarding the personal information that is under the government's control and limiting government interventions into the private lives of Canadians to lawful and necessary purposes

Rights of access and privacy ensure that politicians and bureaucrats remain accountable to the citizenry

## Information Management

Effective management of information provides the foundation for sound management and accountability for the government

It ensures that records are available and that government decisions, including those that directly effect identifiable individuals are based on accurate and up-to-date information

It supports the rights of access to information and access and correction of personal information

## INFORMATION

## Security

Protecting personal information and ensuring its integrity and confidentiality builds trust between citizens and its government

Safeguarding information assets ensures the protection of legal, economic, political and national interests which in turn helps preserve the rights of citizens in a democratic system of government

## Information technology

Efficient, effective, and innovative information technology (IT) is a key enabler to achieving well-managed information in support of policies, programs, and services. transforming the business of government.

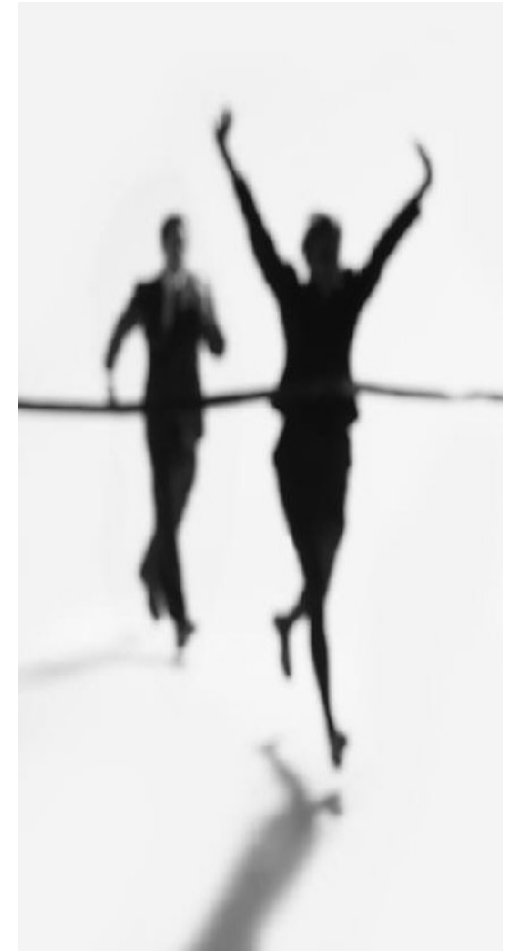
Information technology is an essential component of the government's strategy to address challenges of increasing productivity and enhancing services to the public for the benefit of citizens, businesses, taxpayers and employees.

# ATIP – Phase I

**Policy on Access to Information**

**Policy on Privacy Protection**

**Directive on the Social Insurance Number  
(SIN)**



# ATIP – Phase II

**Directive on the Administration of  
the *Access to Information Act***

**Directive on Privacy Practices**

**Directive on Privacy Requests and  
Correction of Personal  
Information**

**Directive on Privacy Impact  
Assessments**

**Reporting requirements relating to Info Source, Annual Reports  
and Statistical Reports**



# ATIP – Phase III

Supplementary policy instruments relating to:

- Access to Information
- Privacy Protecting



# Emerging policy issues



**Accountability and transparency are increasingly important both domestically and internationally**



**Social media and other new technologies require policy responses to ensure access to information and privacy considerations are respected in the new environment**



# For more information

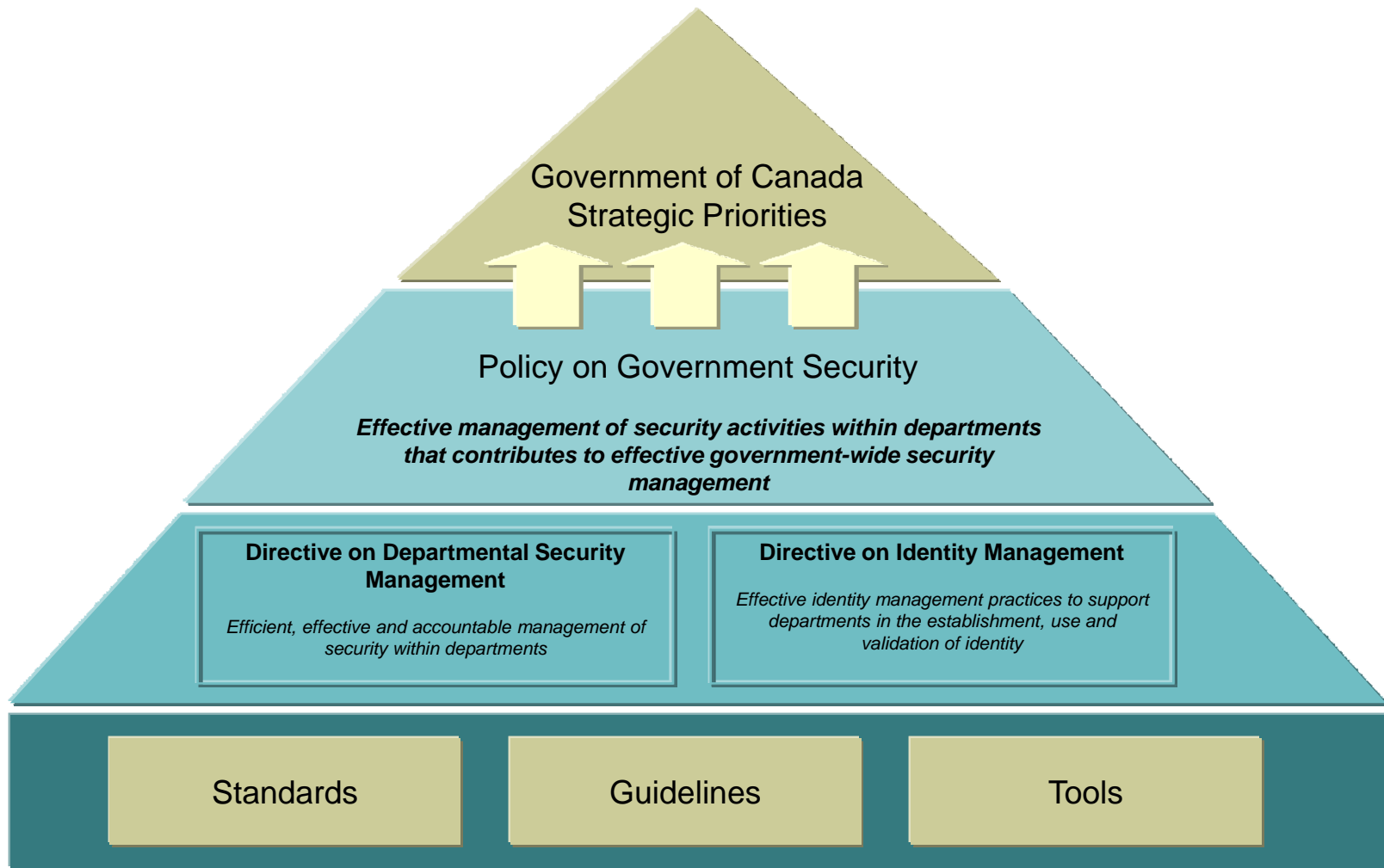
- Policy and directives
  - Policy on Access to Information (<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453>)
  - Policy on Privacy Protection (<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510>)
  - Directive on the Social Insurance Number (SIN) (<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13342>)
- Access to Information and Privacy Web site
  - <http://www.tbs-sct.gc.ca/atip-aiprp/index-eng.asp>
- Telephone: (613) 946-4945
- Email: [IPPD-DPIPRP@tbs-sct.gc.ca](mailto:IPPD-DPIPRP@tbs-sct.gc.ca)



# Agenda

- ATIP & Privacy
- **Security**
- Information Management
- Information Technology

# The goal: Effective government-wide security management





# Current status

- On **July 1, 2009** the Policy on Government Security, Directive on Departmental Security Management and Directive on Identity Management came into effect
- Policies rescinded
  - Government Security Policy (2002)
  - Policy for Public Key Infrastructure Management in the Government of Canada (2004)
- Delegation of authority granted to the President of the Treasury Board to issue and amend directives and standards related to:
  - Information and Identity Assurance, Security Screening of Individuals, Physical Security, IT Security, Emergency and Business Continuity Management, Security in Contracting

# What's new / changed?

- Applies to all departments within the meaning of Schedules I, I.1, II, IV and V of the Financial Administration Act (FAA), unless excluded by specific acts, regulations or Orders in Council
- Roles and responsibilities clarified and aligned to mandates – within departments and government-wide
- Departmental security planning provides integrated view of corporate security risks in relation to departmental priorities
- Identity management as a foundation for trust
- Enhanced requirements for monitoring and performance measurement

**The essential requirements for protecting government information, assets and services against compromise and individuals against workplace violence have not changed and continue to be covered under the policy and suite of directives and standards on security and identity management**



# TBS Support

- **Phased over three years**
  - Phase I: Ensure security awareness<sup>1</sup> and governance
  - Phase II: Support business processes
  - Phase III: Sustain and Improve Performance
- **Five streams of activity**
  - 1) Communications and Awareness
  - 2) Training and Development
  - 3) Governance
  - 4) Standards Development
  - 5) Performance Measurement

1. Overall awareness of roles and responsibilities and policy instruments

# Phase 1 (2009-2010)

## Key TBS support activities

### Communications and awareness

- Message from Secretary and CIO, SPIN, Fact sheets, Q&As on Web
- Awareness sessions (as needed)
- Present at committees, DSO/ITSC meetings, etc.

### Governance (ADM Security and Identity Committees)

- Review Terms of Reference and membership
- Support advancement of work on standards and guidelines

### Standards Development

- Standard on Information Assurance
- Standard on Individual Security Screening
- Guideline on Departmental Security Planning
- Guideline on the Management of Public Key Infrastructure
- Performance Measurement Framework and Key Performance Indicators



# For more information

Web: Policy and directives

<http://www.tbs-sct.gc.ca/sim-gsi/pc-cd/dev-ela-eng.asp>

<http://www.tbs-sct.gc.ca/sim-gsi/pc-cd/dev-ela-fra.asp>

<http://publiservice.tbs-sct.gc.ca/sim-gsi/pc-cd/documents/dev-ela-eng.asp>

<http://publiservice.tbs-sct.gc.ca/sim-gsi/pc-cd/documents/dev-ela-fra.asp>

## Questions and Answers

<http://publiservice.tbs-sct.gc.ca/sim-gsi/sr/documents/qa-qr-eng.asp>

<http://publiservice.tbs-sct.gc.ca/sim-gsi/sr/documents/qa-qr-fra.asp>

Telephone: (613) 946-5046

(613) 957-2549 (IT Security)

Email: [SIDM-SGID@tbs-sct.gc.ca](mailto:SIDM-SGID@tbs-sct.gc.ca)



# Agenda

- ATIP & Privacy
- Security
- **Information Management**
- Information Technology

# GC IM Strategy – Outcomes

## GC Information Management Strategy Outcomes Framework

### MANAGEMENT EXCELLENCE

Delivery of high-value programs, efficiently, transparently, and accountably

GC has the capacity to make effective decisions and deliver on priorities

### ULTIMATE OUTCOMES

#### VISION FOR IM IN THE GC

Information is safeguarded as a public trust and managed as a strategic asset to maximize its value in the service of Canadians

### PRINCIPLES FOR SELECTION & MEASUREMENT OF GC IM STRATEGY ACTIVITIES

Align IM activities

Comply with IM Policy instruments more consistently

Reduce redundancies and duplication in investments

Adopt common or shared IM services

Leverage innovation and expertise

Address IM skills and capacity issues

### STRATEGIC GOALS

#### POLICY & GOVERNANCE

A fully implemented set of policy instruments supporting information management outcomes, defined accountabilities, and effective management of GC information assets.

#### PEOPLE & CAPACITY

A highly-skilled Government of Canada workforce that achieves information management outcomes by applying the appropriate information management policy instruments

#### ENTERPRISE INFORMATION ARCHITECTURE

A fully documented and sustainable set of information architecture services, principles, methods, standards and processes that respond to the information needs of the GC enterprise

#### IM TOOLS & APPLICATIONS

Enterprise information management tools that fully support the business user and that are compliant with the information architecture





# IM Policy

**Strategic Goal:** A fully implemented set of policy instruments supporting information management outcomes, defined accountabilities, and effective management of GC information assets.

## **Priorities:**

- Strengthen information management practices for the Government of Canada
- Enable smarter investments in information management
- Improve stewardship of Government of Canada information assets

# IM Policy Structure

## INFORMATION MANAGEMENT POLICY

### IM Directive

#### Governance & Strategic Planning MAF 12.1, 12.2

Plan    Analysis    Design    Implement    Maintain

#### Standards

- ERP

#### Guidelines

- IM Basics
- IM Planning
- IM Leadership
- IM Practioners

#### Tools

### Recordkeeping Directive

#### Practice MAF 12.3

Create    Distribute    Use    Maintain    Dispose

#### Standards

- Geospatial
- Metadata
- Data Stewardship

#### Guidelines

- Email
- Web 2.0
- Litigation
- Business Value

#### Tools

Plan ---» Design ---» Transform



# IM Policy Development for 2009 - 10

## GC IM Strategy – Year 2

Policy instruments currently in development for delivery this year include:

- Metadata Standard
- Guideline on IM: Email
- Guideline on IM: Web 2.0
- Guideline on IM: Business Value
- Guideline on IM: Litigation



# Next Steps

1. Year 2 Instruments approved for delivery (Spring 2010)
2. Year 3 instrument development started (Summer 2010)
  - Guideline on IM: Practitioners
  - Guideline on IM: Metadata
  - Guideline on IM Internal Services
  - Standard on Data Stewardship

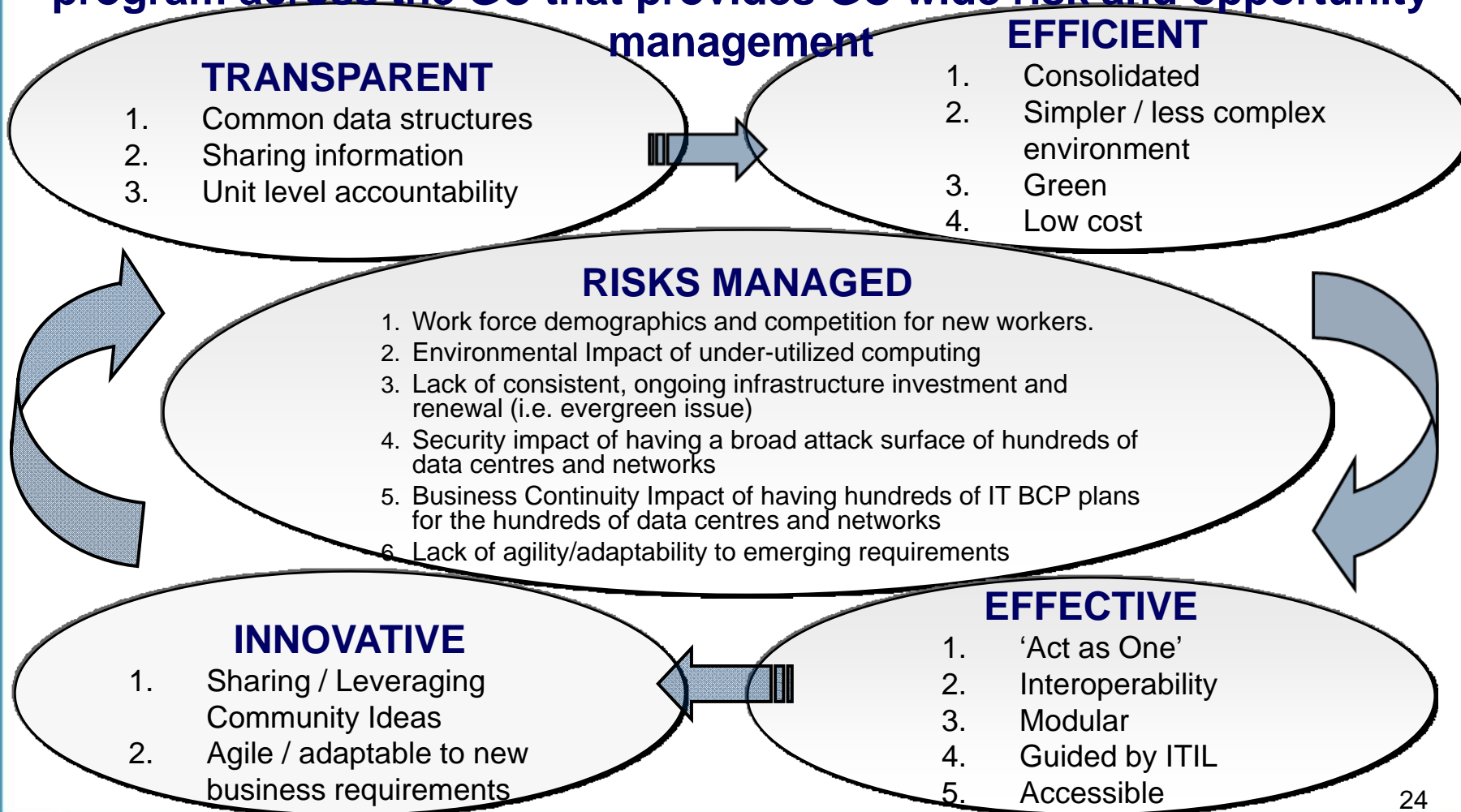


# Agenda

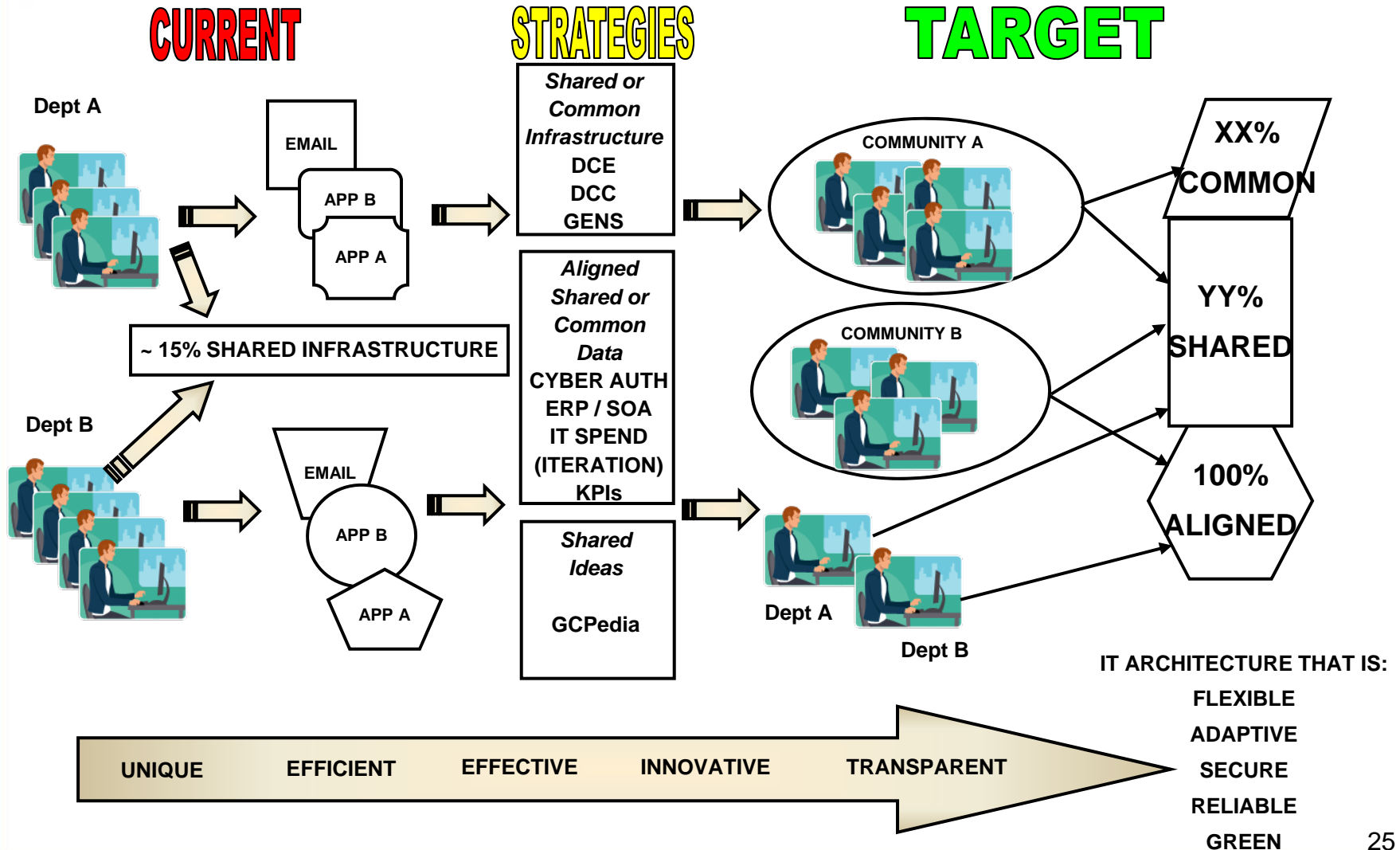
- ATIP & Privacy
- Security
- Information Management
- **Information Technology**

# Result: An Initial GC IT Vision

Collaboratively develop and consistently use an IT Management program across the GC that provides GC wide risk and opportunity management



# GC IT Strategy – An Evolutionary Program



# Policy on Management of IT

Effective management of information technology within departments and government-wide

## Accountabilities of all Deputy Heads:

1. Senior official designated
2. **Participate in setting Gov-wide directions**
3. Governance structures established
4. IT Plan integrated into business plan
5. IT performance measured
6. **Use Common and shared services**
7. Standards development

# Directive on Management of IT

## CIO of Canada & CIO Council Terms of Reference

The CIO of Canada will:

1. Chair the CIOC;
2. Identify members of the CIOC and ensure that participation is commensurate with size of the department;
3. Ensure that there is a collective decision-making process for the Council; and
4. Fund the operations of the CIOC.

Chief Information Officer Council (CIOC):

1. Establish an annual planning cycle that will shape the agenda of the Council;
2. Publish a strategic plan periodically at the discretion of the Chair; and
3. Be responsible for communicating and engaging the GC-wide IT community on decisions, plans, progress, risks and challenges associated with the management of IT and GC IT decisions that will impact departmental operations

# Directive on Management of IT

The Departmental CIO or equivalent has a responsibility to:

1. Developing departmental governance structures for deputy head approval to support effective IT decision making;
2. Co-ordinating, promoting and directing information technology and collaborating on IT-enabled business transformation with the business owner or other stakeholders;
3. Participating in federal government IT governance forums, including the Chief Information Officer Council (CIOC) and other designated governance and advisory forums, on matters related to IT and federal government IT architecture;
4. **Balancing individual departmental interests with government-wide interests to contribute towards government-wide IT directions and strategies;**
5. Advising the CIOC on the decisions, plans, progress, risks and challenges associated with the provision or consumption of common or shared IT services
6. Monitoring and measuring departmental IT management performance using both government-wide and departmental key performance indicators as appropriate;
7. Advising the deputy head, in collaboration with the business owner and other stakeholders, about the effect of new or amended legislation and policies on departmental IT plans.

IT Governance

# Directive on Management of IT

...

## IT Planning

The Departmental CIO or equivalent has a responsibility to:

1. **Developing, implementing and sustaining an effective departmental IT planning process that is integrated with the overall departmental corporate planning process and aligned to the investment planning process to support business, enable transformation and guide IT decision making;**
2. **Preparing an IT plan that describes: governance, IT business, performance measurement and risk management. Provide an annual IT Progress Report on planned activities and submit to TBS (CIOB) on an as-requested basis; and**
3. **Ensuring that the IT plan is aligned to support departmental business and government-wide strategic directions by communicating with and engaging departmental and external stakeholders .**

# Directive on Management of IT

## IT Strategies

The Departmental CIO or equivalent has a responsibility to:

1. Developing and maintaining efficient and effective departmental IT management practices and processes, as informed by ITIL (Information Technology Infrastructure Library) and COBIT (Control Objectives for Information and related Technology), with priority on IT asset management, the IT service catalogue and IT service costing and pricing, as appropriate ;
2. **Aligning departmental IT management practices, processes and technology architecture with federal government IT strategy, directions, standards and guidelines as they become available and as they evolve under the guidance of the CIOC;**
3. Participating, as a service provider or a service consumer, in the conception, planning, evolution and oversight of common or shared IT services and solutions;
4. Developing, implementing and sustaining departmental strategies for producing or consuming appropriate common or shared IT services and solutions, based on the IT plans;
5. Aligning and documenting IT services, planned or currently offered to recipients, according to the Management, Resources, and Results Structure Policy (MRRS). The Profile of GC Information Technology Services provides additional guidance for the alignment and documentation of the IT Services; and
6. Reviewing and assessing IT services periodically to identify opportunities for enhancing efficiency, effectiveness and innovation as determined by governance and in collaboration with service providers, service consumers and other stakeholders.



# Next Steps

## Standard on ERP Usage (Mandatory)

- Join a cluster
- Evaluate moving to GC HRMS or IFMS whenever making significant investment in HR or Finance Systems
- Implement OCHRO and OCG processes

## Parse CLF Standard

## Guideline on Enterprise Architecture (Guidance – but MAFable)

- Endorse TOGAF and align existing guidance documents
- Endorse TOGAF and align existing guidance documents

## Guideline on Industry Standards for IT (Guidance – but MAFable)

- Beginning of ‘how we do things around here’



# Thank-you !

