Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada

DCE Architecture Blueprint

Part 1 - Principles

Public Works & Government Services Canada
Information Technology and Services Branch

Distributed Computing Environment

Canada

Document Version:	1.0, 2nd Release
Document Status:	Final for General Distribution
Date of Issue:	2006.02.03
Document Classification:	

DOCUMENT APPROVAL

	Role	Name	Signature
Approved by:	Director General, Chief Technology Office PWGSC/ITSB	Robert Maynard	Date: _____
Accepted by:	Director General, Service Management & Delivery PWGSC/ITSB	Maurice Chénier	Date: _____
Accepted by:	Director General, Product Management PWGSC/ITSB	Gale Blank	Date: _____
Endorsed by:	Executive Director, Enterprise Architecture and Standards TBS/CIOB	Gary Doucet	Date: _____
Endorsed by:	Senior Director, Technology and Internal Services Strategy TBS/CIOB	Chuck Henry	Date: _____
Recommended by:	DCE Line of Business Executive PWGSC/ITSB	Tom Cockwell	Date: _____

The GC Chief Architect concurs with the intent and direction of the draft DCE Architecture, as a sub-program architecture of the IT-SSO and its plan for community-of-interest feedback. As presented, the draft DCE Architecture generally aligns with the GC-wide level enterprise architecture principles and the GC EA framework comprised of architecture views of business, information, application and technology. Future releases of the document should include incorporating the GC cross-program architecture views for security, privacy and accessibility, as appropriate or they become available.

GC Chief Architect, Gary Doucet
TBS, CIOB, EASD

Document Change Control

Version	Date Issued	Author(s)	Brief Description of Change
0.8	December 6, 2005	T. Peters	The original Architecture Blueprint has been divided into two separate parts: Part 1 - Principles; and Part 2 - Reference Models and Standards. This document has been created based on version 0.5 of the original deliverable and includes recent comments from CIOB (TBS) and CTO (ITSB/PWGSC). This version is for internal team review, including CIOB, prior to final review by the stakeholders.
0.9	December 13, 2005	T. Peters	Incorporated comments from Team Review, including CIOB. Reduced number of and revised IT program-level principles. Added introduction and context as provided by CIOB.
1.0	January 19, 2006	T. Peters	Incorporated final comments from Senior Management of ITSB and CIOB. Deliverable released for general distribution.
1.0, 2nd Release	February 3, 2006	T. Peters	Clarification to Cost Savings in Business Drivers (Section 2.1). Minor edits to Profile of GC IT Services (Section 3.2). Approval not required.

Table of Contents

1 INTRODUCTION

The Government describes "modernizing Government" as acting as one rather than 116 separate departments and agencies[1]. It means simplifying business processes, re-using information and systems, and capitalizing on technology to better manage money and operations. It means using common approaches and shared internal services wherever possible. Introducing more shared systems, simplifying and standardizing processes for these administrative activities, moving routine activities to self-service on the Internet, and shared service delivery will result in efficiencies.

The Government of Canada (GC) is implementing a strategy to improve the delivery of these internal administrative services and increase operational efficiency. Building on the areas of greatest opportunity, the Government is advancing a shared service approach to information technology (IT), human resource management, and financial services starting with a critical mass of departments and agencies. In this way, decision-making is improved, costs reduced and resources saved. Greater operational efficiency means more available funding for Canadians' highest priorities.

The draft Profile of GC IT Services[2] outlines a common view of the GC's IT Service domains that include:

- Distributed Computing,
- Application Development and Maintenance,
- Production and Operations Computing,
- Telecommunications Network – Data & Voice, and
- IT Security.

1.1 DOCUMENT PURPOSE

The purpose of the DCE Architecture presented is to establish a framework that guides the engineering, implementation and delivery of the DCE service offerings, informed and aligned with GC-level and IT Program-level (and SSO) enterprise architecture views. In developing the DCE Architecture Principles, a series of principles for the Program level architecture for IT emerged and are presented as a provisional draft set of IT Program-level architecture principles for discussion and review by appropriate stakeholders and the TBS CIOB OPI.

The DCE Architecture Principles have been created in consultation with the Chief Information Officer Branch (CIOB) at Treasury Board (TBS) and reviewed and validated by the DCE Architecture Advisory Committee (AAC) and the DCE Thought Leadership Forum (TLF). The AAC is comprised of Architects from nine Government Departments and Agencies, representatives from other lines of business within the Product Management Sector in

[1] Reference Budget 2005.
[2] Draft Profile of GC IT Services, version 1.9, dated July 2005.

PWGSC/ITSB, as well as representation from Enterprise Architecture and Standards Division (EASD) of TBS/CIOB. The TLF is made up of representatives at the CIO level from twenty-two Government Departments and Agencies and is responsible for strategic thinking and planning with respect to DCE service offerings.

1.2 DOCUMENT AUDIENCE

The primary audiences for this document are the Chief Technology Office, Product Management and the Service Delivery & Management Sectors of PWGSC/ITSB and Treasury Board (CIOB). Additional audiences for this document include other Government Departments and other organizations within PWGSC.

1.3 CONTENT OF DOCUMENT

The IT-SSO/DCE Architecture presented consists of:

- Positioning the DCE architecture within the GC Enterprise Architecture framework;
- An overview of the (draft) Profile of the GC's IT Services;
- Key business drivers for the Program-level IT (and related SSO) and DCE architectures and their associated strategic requirements as the basis for formulating architecture principles; and
- A cascading set of architecture principles, derived from these key business drivers, that are aimed at guiding the engineering and implementation of Program-level IT (and SSO) / DCE services.

2 DCE BUSINESS DRIVERS AND COMMON STRATEGIC REQUIREMENTS

Architectures are based upon an accepted set of business needs: the motivation factors and case for action. The current state of distributed computing in the GC comprises numerous different desktop operating systems, office productivity suites, electronic messaging servers, independent (and sometimes conflicting) directories, security tools and policies, file servers, network operating systems, remote access tools, etc. Most such tools are present in multiple versions and many do not interface with each other, internally with departmental business/program applications, or externally with other government departments.

2.1 DCE BUSINESS DRIVERS

A business driver is a business factor that is a primary motivation for the solution under development and against which the solution will be evaluated. The key business drivers, as defined in the Business Case for Enterprise IT Services, for the Shared Services initiative in general and the DCE component in particular are as follows:

1. **Cost Savings:** Reduce IT spending for DCE services by 10 to 20% over 5 years through common (and shared) service delivery;
2. **Enterprise Wide Approach:** The delivery of Distributed Computing services in holistic and common approach, aligned with the GC Enterprise Architecture;
3. **Client Service Focus**: Deliver standard, consistent measurable and less complex shared services across the enterprise taking advantage of the economies of scale that this offers; and
4. **Business Transformation Enablement**: The GC is currently rationalizing the way it delivers services to Canadians and consolidating Departmental delivery interfaces into fewer client facing organizations and leveraging common IT services.

2.2 COMMON STRATEGIC REQUIREMENTS

2.2.1 COST SAVINGS

The resources being allocated to IT services are not being used in the most efficient and effective way to deliver optimal results to the GC. The substantial investments and ongoing expenditures devoted to these areas need to be managed with a view to maximizing the overall value to the taxpayer and service to the client (an Enterprise Approach).

In the current environment IT Services are, for the most part, being delivered by individual Departments, resulting in significant duplication of effort and increased costs across the GC. Significant opportunities for efficiencies and savings can be realized if the service delivery model is changed to an Enterprise or government wide approach. Once fully implemented, there are potential opportunities for savings in the order of 10-20% for the delivery of Government wide DCE Services.

2.2.2 ENTERPRISE WIDE APPROACH

In the current environment Government of Canada Departments and Agencies behave as individual entities. This “siloed” approach serves as an inhibitor to achieving cost effective and consistent IT service delivery. The inefficiencies and complexities introduced by continuously and repetitively having to integrate shared business objectives across multiple IT infrastructures drives up cost and extends time-to-delivery. Overall management practices need to be more robust and more mature in order to prevent unnecessary duplication and to optimize service delivery from a GC perspective.

Private sector and other Governments faced with the same situation as the GC are addressing the situation through the aggressive pursuit of enterprise-wide architecture and common IT service delivery solutions. Results have proven that a common approach to delivery of services allows organizations to consistently implement policies and standards such that service delivery is enhanced while cost of delivery is reduced.

2.2.3 CLIENT SERVICE FOCUS

As a critical enabling tool for the transformation of Government services to better serve citizens, IT infrastructure and services need to be structured in such a way as to enable a citizen-centric view and to provide transparency with respect to costs and outcomes. Internally this would require end-to-end integration across the Government of Canada enterprise.

Stakeholders, both the general public and the consumer Departments, require improved enterprise-wide IT service delivery with consistency, standardization, and centralization of process along with multiple levels of services supported on a government-wide basis and driven by client business needs.

2.2.4 BUSINESS TRANSFORMATION

The Government of Canada is continuously evolving the programs and services it delivers to Canadians. The scope of a particular business transformation may be within a Department but more often spans multiple Departments. An example of a very significant business transformation is the Service Canada initiative. This initiative was established in 1999 by Treasury Board Secretariat (TBS) as a pilot project with a mandate to provide Canadians with one-stop access to the services of the "whole of government", and to deliver those services in a fast, reliable, convenient and cost effective manner.

In order to enable services, such as those delivered through Service Canada, a solid foundation is required - specifically a common IT Infrastructure that spans the departments providing citizen facing services. The DCE LoB will establish core components of this IT foundation that Departments can leverage for program delivery.

3 DCE VISION & PROFILE OF IT - DCE SERVICES

3.1 DCE VISION

The vision of the Distributed Computing Environment (DCE) line of business is to develop a set of utility services, which all Government Departments and Agencies will use. Distributed computing refers to the entire complex distributed desktop environment, including the supporting foundational services. A DCE utility service will enable the GC to:

1. Reduce its operating and procurement costs;
2. Align its Distributed Computing service into a common target environment for which Business/Program applications can be developed and implemented across-Government;
3. Enable Enterprise Service Management, data exchange, patch management; and
4. Establish a single provider responsible for the delivery of the entire service to Government.

3.2 (DRAFT) PROFILE OF GC IT SERVICES

The following excerpt has been taken directly from the Profile of GC IT Services, GC Enterprise Architecture – Profiles version 1.9 published by TBS/CIOB in July of 2005:

The Profile of GC IT Services as highlighted in the following table, outlines the most common sets of GC IT services for five main IT service groups: Distributed Computing, Application Development and Maintenance, Production and Operations Computing, Telecommunications Network – Data & Voice, and IT Security.

IT Services Groups	*Profile of GC IT Services*
Distributed Computing	*Standard Desktop and Office Productivity Suite*
	Electronic Messaging and Workgroup (Collaboration) Services
	GC Corporate Administrative / Program-Specific Applications
	File/Print Service
	Remote Desktop Delivery Service
	Logical Access Directory Service
Application Development & Maintenance	*Applications Development Services*
	Deployment Services
	Integration Services
	Engineering and Testing Services
	Certification/Release Services
Production and Operations Computing	*Midrange Computing Services*
	Mainframe Computing Services
	Dedicated Application Hosting & Management Services
	Facilities Management Services

IT Services Groups	*Profile of GC IT Services*
Telecommunications Network – data, voice	*Network Management and Operations Services*
	Connectivity Services
	Data Network Services
	Voice Network Services
IT Security	*Physical Environment Services*
	Identification, Authentication, Authorization Services
	Detection, Response, Recovery, Audit Services
	Perimeter Defence Services

Table 1 - Summary of GC IT Services

3.3 PROFILE DESCRIPTION OF GC IT / DCE SERVICES

Expanding the Distributed Computing Services grouping[3], TBS/CIOB defines the following:

Distributed Computing Services includes the provision and support of workstation hardware (e.g. PC, notebook) and the set of capabilities that support office productivity suites, email and calendaring, browser, anti-virus and common utilities, etc. This service also provides the capabilities that support work group communications, corporate administrative and program-specific applications, directory services, file and print services, remote access services, local network operating systems, locally attached peripherals, and the local interconnectivity provided through Local Area Network (LAN) technologies.

- ***Standard Desktop and Office Productivity Suite:*** *provides the set of capabilities that support the underlying capabilities to access and use IT systems, including: the physical hardware (desktop computer, notebook computer, PDA), the Operating System, Internet Browser, Corporate Portal: and standardized office suites for word processing, spreadsheets, presentations, databases, and standard utilities such as anti-virus, security, data handling tools, and client-side printing utilities.*

- ***Electronic Messaging and Workgroup (Collaboration) Services:*** *provides the set of capabilities that support e-mail, scheduling services, and workgroup applications and includes: internal and external e-mail transmission/receipt, government-wide calendaring/scheduling; and the capabilities for workgroup collaboration facilities such as controlled public-access/shared folders, workgroup information sharing, bulletin boards, electronic forums, and community of interest workspaces.*

- ***GC Corporate Administrative / Program-Specific Application Services:*** *provides the set of capabilities that support Program-specific and corporate administrative applications enabling service delivery, administration, management, information management and decision-making activities.*

[3] Draft Profile of GC IT Services, version 1.9, dated July 2005.

- ***File/Print Service:*** *provides the set of capabilities that support user/group access for the storage, retrieval and protection of office-type documents such as word processing, spreadsheets, presentations, and data files; and shared workgroup folders. The Print service acts as the "server-side" of the printing service and provides the capabilities for handling all "local" print requests submitted from desk top applications.*

- ***Remote Desktop Delivery Service:*** *provides the set of capabilities that support remote end-users with complete access to the standard Distributed Computing Desktop components, applications and data via access over a Secure Remote Access, Dial-in or wireless service such as those offered through the Data Centre service.*

- ***Logical Access Directory Service:*** *provides the set of capabilities that support identity/group-based privileges to users who require access to Distributed Computing systems, data and/or printers. As a single sign-on directory, the Logical Access Directory is responsible for ensuring that only the information granted for users to view is accessible (e.g. e-mail, databases, information holdings, and/or applications).*

4 ARCHITECTURE PRINCIPLES

In light of the strategic business drivers and strategic requirements presented, the following outlines a vision, service profile and cascading set of architecture principles that aim to guide the planning, engineering, implementation, delivery and support of DCE and associated shared services to be provided through the IT-SSO.

The GC Enterprise Architecture:

- At the GC-level provides artifacts that guide the consistent design and engineering of business services and processes, information and technology systems – government-wide;
- Informed and guided by the GC-level architecture, the Program and SSO level Architectures like IT / DCE are extended with increasing level detail and will typically include guiding principles, best practices and models that guide the engineering and implementation of these respective Program or SSO services and solutions.
- Program / Department level architectures will include policies, principles and best practices for engineering and implementing specific department solutions; and
- SSO Program level architectures will typically include the policies, principles and best practices that guide the design, delivery and support of shared services to be provided to client Departments, as well as policies and principles for use of shared services.

Figure 1 graphically presents the cascading of Principles from the Enterprise (GC) level, to the Program (IT) level down to the Project or Line of Business (DCE) level. The resultant set of Principles which apply to the DCE LoB are the sum of GC, IT and DCE levels combined.

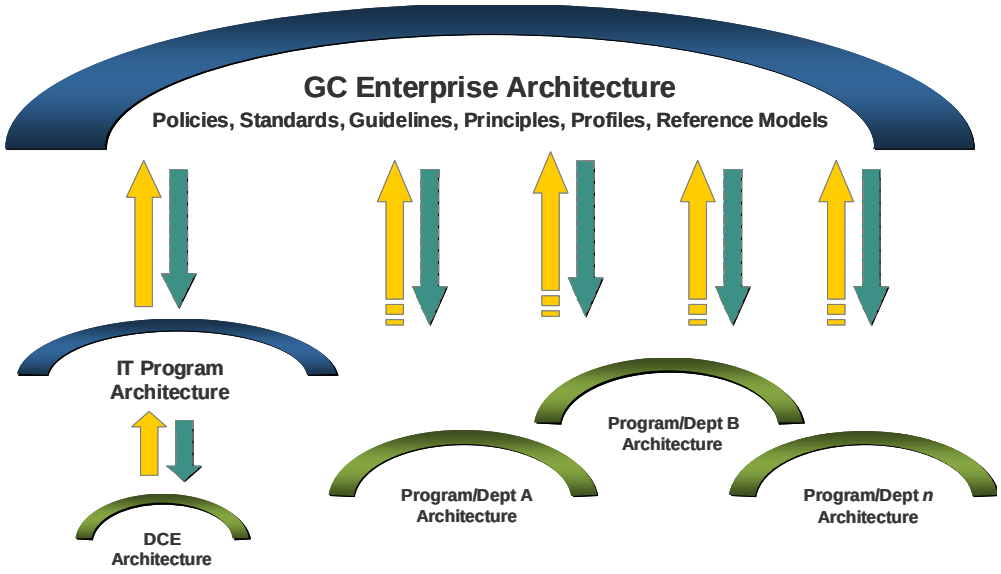

Figure 1 - Architecture Context

4.1 GC-LEVEL ARCHITECTURE PRINCIPLES[4]

4.1.1 GC PRINCIPLE 1: REDUCE INTEGRATION COMPLEXITY

The federated architecture must promote reduced complexity and enable integration to the maximum extent possible. We must re-engineer application systems to be "highly modular" and "loosely coupled" to be able to reuse components.

4.1.2 GC PRINCIPLE 2: HOLISTIC APPROACH

Information is a government asset. Its value is enhanced when it can be accessed and applied to accelerate decision making, which is leveraged through interdepartmental collaboration within the bounds of legislation and privacy. The infrastructure must promote a "whole of government" approach while respecting unique federal government roles and mandates.

4.1.3 GC PRINCIPLE 3: BUSINESS EVENT-DRIVEN SYSTEMS

Systems must be designed to be business event-driven. This principle applies to manual, process and application systems. Further, application systems must keep the operational data necessary to allow the government to re-create any business event.

4.1.4 GC PRINCIPLE 4: DEFINED AUTHORITATIVE SOURCES

All information must have defined "authoritative sources." These sources will act as information stewards. Authorized data must be accessible and available for re-use by any entitled systems and/or business process.

4.1.5 GC PRINCIPLE 5: SECURITY, CONFIDENTIALITY, PRIVACY AND PROTECTION OF INFORMATION

IT systems must be implemented in adherence with government security, confidentiality and privacy policies and laws. Information must be protected against unauthorized access, denial of service, and both intentional and accidental modification.

[4] The Enterprise Architecture and Standards Sector of CIOB at TBS has published iteration one of the Federated Architecture Program that defines the IM/IT related components of the GC Enterprise Architecture. The document is currently being revised however the principles defined therein are still applicable to the DCE line of business. These principles are imported directly from the FAP document available on the TBS website and are inherited by the DCE program architecture. The titles of the principles have been changed slightly for clarity; GC has replaced Architecture. For principle rationale and implications, please refer to the official document.

4.1.6 GC PRINCIPLE 6: PROVEN STANDARDS AND TECHNOLOGIES

IT solutions must use commercially viable standards-based technologies. The customization of purchased software must be avoided wherever possible. Priority will be given to products adhering to industry standards and open architecture.

4.1.7 GC PRINCIPLE 7: TOTAL COST OF OWNERSHIP (TCO)

Total Cost of Ownership for applications and technologies (hardware and software) must balance development, support, disaster recovery and retirement costs along with the costs of flexibility, scalability, ease of use/support over the life cycle of the technology or application.

4.1.8 GC PRINCIPLE 8: PLAN FOR GROWTH

IT must plan, design, and construct for growth and expansion of services (known requirements) across government.

4.1.9 GC PRINCIPLE 9: ADOPT FORMAL METHODS OF ENGINEERING

Government must employ formal practices, methods, and tools for architecture and engineering for all stages of these disciplines in IM/IT, from design to implementation and construction.

4.1.10 GC PRINCIPLE 10: EXTENDED INFORMATION AND SERVICES ENVIRONMENT

To the extent possible, the integration of the IM/IT infrastructure must enable the provision of Government of Canada information and services to citizens, businesses, and other governments (i.e. provincial, municipal and international).

4.1.11 GC PRINCIPLE 11: MULTIPLE DELIVERY CHANNELS

Support client delivery channel preferences in accessing government services.

4.1.12 GC PRINCIPLE 12: ACCESSIBLE GOVERNMENT

To be responsive to the increasing diversity of Canadian society, the Government of Canada must be accessible to all citizens.

The following are sub-principles related to universal design to be applied in the architecture and included in the IM/IT infrastructure by Core and Domain architecture teams:

Equitable Use: *Accommodating all users in relation to electronic networks. This means that delivery of services must occur simultaneously for all accessibility needs.*
Flexibility of Use: *While promoting a degree of standardization and compatibility with various electronic information technologies, accommodating a wide range of individual preferences and abilities.*
Simple and Intuitive Use: *Ensuring ease of comprehension and use, regardless of the user's experience, knowledge, language skills, or concentration level.*
Perceptible Information: *Communicating information effectively, regardless of the user's physical and/or sensory abilities, so that it can be used efficiently and comfortably with a minimum of fatigue.*

4.1.13 GC PRINCIPLE 13: ROBUSTNESS

Implemented infrastructure must be robust, responsive, and reliable with appropriate redundancy to protect against system failure.

4.2 IT PROGRAM-LEVEL ARCHITECTURE PRINCIPLES

The IT Program Domain has yet to be defined in terms of its Enterprise Architecture including the definition of over arching principles, which apply to all GC IT services regardless of whether they are delivered through the ITSSO or not. The following principles have been established, from the ITSSO perspective, as suggestions for the IT Program-Level and will be discussed and finalized with TBS CIOB Technology and Internal Services Strategy.

4.2.1 IT PRINCIPLE 1: LEVERAGE ECONOMIES OF SCALE AND EXISTING INVESTMENTS

The GC, acting as an Enterprise, has an overwhelming opportunity to leverage economies of scale particularly in the area of procurement. By standardizing procurement across the GC Enterprise for common IT elements, the GC will be able to realize cost savings almost immediately and buying more for less. This principle also supports the focus on shared service delivery elements and standardization across the GC. In addition, leverage existing investments made by client Departments in assets and services utilized in the delivery of IT services. These existing investments may be extendable to the GC, reducing the requirement(s) for acquisition.

Rationale:

Leverage economies of scale and leveraging existing investments will allow IT services to:

- Reduce purchase costs driven by GC wide volume and/or existing vehicles;
- Reduce acquisition timeframes given some products and/or services may be pre-existing;
- Reduce Support cost driven by product standardization across the enterprise; and
- Reduce administrative costs, competing and managing the vehicles.

Implications:

- Major changes to procurement – will require industry consultation and competition (RFPs); and
- Implementation will require a robust and scalable GC wide IT asset management solution.

4.2.2 IT PRINCIPLE 2: REDUCE IT COMPLEXITY

IT Complexity will be dramatically reduced for the Government of Canada as an Enterprise by providing common services. A single service provider with limited variations or 'few flavours' of service offerings will deliver these services.

Rationale:

Reducing IT complexity will allow lower 'Total Cost of Ownership' for the Government of Canada as an Enterprise.

Having a single service provider will streamline many aspects of IT, allowing economies of scale to be established by the provider.

Limiting permutations of the offering will continue to keep TCO down by streamlining the support and administration effort.

Implications:

The ITSSO will be a single service provider for shared IT services. This will reduce configuration options that Departments currently have for delivery of such services.

Having a single service provider and few flavours of service will allow the Infrastructure to be better managed through change to meet emerging needs of the Enterprise (more adaptable and flexible as a whole).

4.2.3 IT PRINCIPLE 3: ENSURE SERVICE FLEXIBILITY

Departments and Agencies of the GC deliver diverse services to their constituents, both internally and externally. ITSSO shared services must have the flexibility to meet these diverse business needs whilst maintaining a standard approach to their delivery.

Rationale:

IT plays a key role in the delivery of services to Canadians, to partners, and to other Government bodies to the point where IT is inherent in business processes. When the ITSSO assumes

responsibility for the delivery of IT services, it must be ensured that business processes and the delivery of services they manage are not interrupted or negatively affected.

Implications:

The ITSSO must perform due diligence from the business perspective and understand how client Departments use IT to enable their business processes and services.

There may be situations where Departmental business processes may change, requiring investment jointly between the ITSSO and the Department.

4.2.4 IT PRINCIPLE 4: LEVERAGE FEDERATED GC IDENTITY

In coordination with other directory service providers establish a federated identity for all employees, contractors and partners of the GC. This identity will provide for Federated:

- Physical access to facilities;
- Secure (PKI enabled) access to electronic resources including network, applications, services, data, etc.;
- Integration with GC Enterprise applications such as Finance and Human Resources;
- Integration with Departmental corporate and business line applications; and
- Synchronization across many directory sources, including password rationalization.

Rationale:

Employees, and others, of the GC currently maintain many different sets of credentials that are used for many different reasons. These credentials are, for the most part, not synchronized and cause much frustration for the user community. This situation is viewed as complex and unnecessary. Also, as sets of credentials increase, calls to Departmental helpdesks increase.

The disparate directories create barriers to the sharing of IT Infrastructure, Information and Applications both between and within departments. The lack of a common GC wide directory service increases the difficulty of implementing change, including the introduction of new services.

Implications:

Rationalizing directory services across the GC will provide for the much-needed direction around application development, specifically the APIs used for authentication. Additionally, this exercise will establish and enforce GC naming standards for directory objects, including users, networks, computers, applications, etc..

Another benefit is that of directory-enabled networking. Networks (wired or wireless) within the GC and/or external can use the common directory service to authenticate devices, users, and

applications and provide the appropriate level of service(s) given the security of the network zone.

4.2.5 IT PRINCIPLE 5: ESTABLISH (AND IMPLEMENT) TIERED STANDARDS AND POLICIES

There is a need to rationalize standards and policies across Government Departments. Treasury Board published policies and standards will be the minimum standard. The solution will provide for two additional tiers of policy (and, potentially, standards) implementation. Each tier will evolve from the previous such that policies are easily managed across the service offerings (i.e. Tier 1 = TBS, Tier 2 = Tier 1 + *x* and Tier 3 = Tier 2 + *y*). Key areas will include:

1. Security (MITS);
2. Records Management;
3. Information Management; and
4. Business Continuity and Disaster Recovery.

Rationale:

Delivering services in an enterprise-wide approach affords the opportunity for improvements in terms of cross-Departmental consistency, standardization, and centralization of standards and policies.

Implications:

Rationalizing the many different policies and standards across the Departments with those published by Treasury Board will require a significant amount of effort. Further establishing the second and third tiers of policy and standard implementation will require some give and take from the Departments and the ITSSO.

4.2.6 IT PRINCIPLE 6: SERVICES MUST BE MEASURABLE AGAINST KEY PERFORMANCE INDICATORS

In support of the Balanced Scorecard, or other business measurement system, and to demonstrate improvements in service delivery, key performance indicators (KPIs) – both internal and external – must be established for each IT service so that SLAs can be created and reported against over time. Each service developed within the IT Program must provide the capability to be measured against these SLAs and more specifically, the KPIs.

Rationale:

Every SLA has KPIs identified when measured and balanced against the SLA targets indicate delivery performance. KPIs are required to establish a baseline by which the ITSSO will measure its all round performance. KPIs are also used on a more frequent basis by Operations to assess actual service delivery versus planned. These KPIs referenced against industry standards

will also be critical for the ITSSO to demonstrate success and establish a continuous improvement program.

Implications:

The GC needs to establish key performance measurements and their target values. This will require a significant amount of effort using a Departmental collaborative approach and may need Treasury Board influence. In addition, the ITSSO must define its business strategy and objectives before the KPIs to measure it can be identified.

4.2.7 IT PRINCIPLE 7: INCLUDE SERVICE CAPABILITY FOR CROSS JURISDICTION UTILIZATION

Many Departments collaborate with or deliver services to different levels of Government in Canada. IT Services must not restrict this capability.

Rationale:

The primary business of the GC is to deliver its core services to Canadians. Impacting service delivery is not an option and considering the ITSSO is the mandated organization to provide IT infrastructure services on which these programs reside – it is imperative that the ITSSO not restrict this functionality.

Implications:

The foundational elements in the ITSSO service portfolios must consider the cross jurisdiction requirements for service delivery. This will require some investment.

4.2.8 IT PRINCIPLE 8: STORE ALL BUSINESS DATA IN A GC SANCTIONED DATA CENTRE

Considering the security and privacy requirements of the Government and the data associated with such, all IT Services must store GC business data within a GC sanctioned Data Centre.

Rationale:

In order to control, manage and integrate the information, records, security and privacy management requirements effectively across the GC, data must be accessible to, in fact hosted by the ITSSO.

Implications:

This principle implies that GC sanctioned data centres are able to deliver Enterprise Storage Services.

The migration of data during the transfer/transform phase of the ITSSO implementation will be extensive. Developing a detailed migration plan while abiding by security and privacy policies will require focused Engineering effort.

4.2.9 IT PRINCIPLE 9: ESTABLISH SERVICE ORIENTED VIRTUALIZED ARCHITECTURE

The ITSSO services portfolio must be designed as an IT Utility such that services are delivered to clients without concern of where, how and what is required behind the scene. When clients purchase a shared service, they receive all aspects of that service, e.g. the DCE Common Desktop service will not only include a workstation tailored to job function but will also include patch and lifecycle management services and support.

Rationale:

The principle is based on the 'virtualization' of end user services. Client departments will sign up for services delivered to key performance indicators. From what and where these services are delivered will be transparent to the clients. This allows the ITSSO to start consolidating service delivery locations without impacting service delivery and further streamline product implementations lowering complexity and cost.

Implications:

Delivering shared (utility) services requires close collaboration between groups, the ITSSO must be formed with proper roles and responsibilities defined. The mindset of the ITSSO must be one of an IT Utility – this is a significant shift from today.

4.2.10 IT PRINCIPLE 10: ENABLE TIERED SERVICE OFFERING

The mandate of the ITSSO is to provide shared IT services to the GC, across many different Departments and Agencies. While flexibility is important in the ITSSO service definition, there needs to be a tiered service offering such that Departments can select default services based on their business needs. ITSSO services will be engineered to a tiered model.

Rationale:

Departmental business needs will drive service adoption and selection. Offering more default options to the GC will aid in establishing the ITSSO as an enterprise service provider. Flexibility is a core requirement for the services offered from the ITSSO.

Implications:

Clear definitions must be established for each of the services being offered from a feature and SLA perspective across the ITSSO. Standardizing on the names of the tiers and their costing/pricing structure will need to be done. The Service Catalogue may need to be modified to present the ITSSO service offerings in their tiers.

4.2.11 IT PRINCIPLE 11: PROVIDE FOR MULTIPLE ADOPTION CHANNELS

Shared IT services will be available to client Departments via four adoption channels in order to provide for Departments to migrate at their own rate. The adoption channels are:

1. Organic Growth (from existing ITSB provided services);
2. IQTT (transformation via waves);
3. Adoption (specific product requests); and
4. Partner and Leverage (strategic partnership with large Department IT transformation).

Rationale:

Some Departments are ready to transfer all of their IT resources and services to the ITSSO, some aren't. Given their respective business reasons, Departments required the ability to adopt shared IT services at their own rates. Each of the four channels provides for a different rate of transformation all of which provide the ITSSO to foster its capability and capacity.

Implications:

Providing different adoption rates, through the channels, may prevent the ITSSO to grow as quickly as it needs to and reach the scale of an enterprise shared service provider.

The development of the capability, both business and technical, must be closely managed to insure that the service is engineered with these channels in mind.

4.2.12 IT PRINCIPLE 12: ESTABLISH COMMON SERVICE MANAGEMENT PROCESSES

IT Service Management (ITSM) processes are a core component to efficient IT service delivery, even more so when services are delivered through an ITSSO. Establishing common, repeatable and efficient ITSM processes will allow the ITSSO to achieve its service delivery goals and objectives. There may be opportunities across the GC to leverage what client Departments have already established and evolve these processes to meet the needs of the ITSSO. It is anticipated that ITIL will form the foundation of these processes.

Rationale:

Developing a set of common service management processes will allow the ITSSO to deliver efficient shared IT services across the Government. They will be well understood and repeatable so as to provide the ITSSO with the flexibility it requires to adapt to Departmental needs.

As a best practice, ITIL should be used as the foundation as it is an industry recognized framework for IT service management. Many public and private sector organizations have invested heavily in establishing these and are benefiting from such.

Implications:

There are many ITSM processes required for the effective delivery of ITSSO shared services. Priority needs to be established and delivery timelines synchronized.

4.3 DCE ARCHITECTURE PRINCIPLES

Each line of business within the ITSSO will have its specific architecture principles that apply to their respective service offerings. The DCE line of business has established the following set of principles at the program level. Some of these principles may apply to other lines of business and may eventually become IT Program principles.

4.3.1 DCE PRINCIPLE 1: RIGHT SIZE AND STANDARDIZE CLIENT ACCESS DEVICE

Right sizing the client device ensures that each client will receive the proper device to perform his or her job function – and that device will be managed through an ever-greening solution.

Standardizing the client device will allow for the ITSSO to manage fewer device profiles. It will further enhance the ability to perform mass procurement that through economies of scale, result in lower cost.

Rationale:

Assignment of standardized client devices will be based on needs and roles. Each client will have the proper device for his or her job function. This will include providing portable devices (notebook computers) for clients with mobility and remote access needs. This will lower total costs by reducing the number of users with multiple computers and associated software requirements.

This will also facilitate the application testing requirements of the service delivery interface, whereby fewer configurations require less time and effort to test.

Implications:

- In the long term the total number of client devices will be reduced across the GC (by device convergence)
- Assignment of devices based on roles and within an ever-greening solution will allow the automation of acquisition workflow and approvals – reducing the manpower required in the authorization process

4.3.2 DCE PRINCIPLE 2: ESTABLISH A STANDARD USER INTERFACE BASED ON JOB FUNCTION

Users across the GC have commented in many different forums that the platform – hardware, operating system (OS) and application(s) – used to perform their job function is far too complex. Client access devices will be designed and assigned based on job function with a standard OS image. Users will be assigned one (1) device. Layered applications will be published according to job function. Finally, all DCE services will be accessible via a standard Internet Browser.

Rationale:

In an effort to reduce complexity, increase resource productivity and ease the transfer of resources within and across Departments – the DCE service offerings will be delivered in a common and easily accessible fashion. This will reduce the need and ultimately the cost of re-training resources.

Implications:

It will be difficult to curb the adhoc IT spending which is very common in the GC today. This may result in non-standard configurations and could impact service delivery. Additionally, application owners must be provided with development standards and API sets so as to begin developing to a Browser based presentation layer.

Interfaces must also adhere to Canada's Officials Languages and Accessibility policies.

4.3.3 DCE PRINCIPLE 3: SUPPORT PROTECTED B DATA

Internal Departmental file and messaging services currently support the use, storage and transmittal of Protected B data (and below) within their organizations. This must be preserved, at a minimum, within the shared services model.

Rationale:

In order for a Department to adopt a shared service it must support the same level of data sensitivity as their current solution. Internal to Departments, Protected B data is stored and transmitted across their infrastructure.

Implications:

Data segregation between Departments may be required to insure that only like-Department information is stored and accessible from a specific data volume. Security controls and data transmission paths must be considered during the detailed design phases. The Government Security Policy (and MITS) must also be considered.

4.3.4 DCE PRINCIPLE 4: PROVIDE FOR MULTIPLE CONNECTIVITY SCENARIOS

There are many design decisions that are influenced by the availability (amount and latency) of network bandwidth. Network availability versus component installation (and management) must be balanced during the Engineering phase. Mobile users must have the ability to work while not connected to the GC network resulting in the provision of data synchronization once re-connected.

Rationale:

In some remote locations within Canada and abroad, bandwidth availability (amount and latency) becomes scarce and expensive. Meeting the goals of maintaining service delivery performance and lowering costs can become prohibitive in this situation. DCE must provide for service provision to a mobile and/or telework workforce.

Implications:

A detailed end-to-end network analysis must be performed for each client Department before DCE services are implemented. There may be a need to define an intermediary storage component for some (i.e. file services) DCE services. The ability to work offline, i.e. not connected to the GC network, with the ability to synchronize data once re-connected must be offered for most, if not all, DCE Services.

4.3.5 DCE PRINCIPLE 5: BUILD IN DISASTER RECOVERY

When consolidating service delivery to fewer physical locations, it is important to engineer disaster recovery, redundancy and fault tolerance into the solution where possible. DCE services will be engineered to minimize single points of failure in the assets of the service chain.

Specifically, each DCE Service Delivery Location (SDL) will be assigned a supporting location such that no physical location presents a single point of failure in the service chain. Supporting location assignments should be done in a fully meshed model such that a single event – natural or otherwise – does not affect both locations.

Rationale:

Maintaining service delivery performance in the area of availability mandates that redundancy and fault tolerance are compulsory requirements of the solution. Business continuity requirements drive further requirements for disaster recovery.

Establishing a replica site for each primary delivery location will allow the ITSSO to meet stringent availability metrics and lower its service delivery risk.

Implications:

Technologies are available to alleviate single points of failure however may introduce significant costs to the solution. Disaster recovery, fault tolerance and redundancy requirements must be analyzed with both benefit (value of the safeguard) and cost in mind.

Real-time data replication products, tools and processes must be analyzed, tested and implemented to meet this requirement. Two primary focus areas are data integrity and network impact.

Data replication across the network can require a significant amount of bandwidth. Real-time replication compounds this requirement.

4.3.6 DCE PRINCIPLE 6: SATISFY INFORMATION AND RECORDS MANAGEMENT REQUIREMENTS

Information Management and Records Management is an important component of the DCE service stack and GC service delivery as a whole. DCE services must be engineered to satisfy the applicable IM and RM requirements.

Rationale:

Government service delivery requires that data related to those delivery programs be properly managed, retained and/or shared within GC facilities. The some services within the scope of DCE, provide storage and management mechanisms for program delivery. IM and RM requirements apply to the new ITSSO shared services.

Implications:

Information and Records Management requirements need to be documented and understood. An integrated solution needs to be developed - with client acceptance and subsequent end-user training.

4.3.7 DCE PRINCIPLE 7: PUBLISH SERVICE APPLICATION PROGRAMMING INTERFACES AND DEVELOPMENT STANDARDS

Application programming interfaces (APIs) and development guidelines must be made available for the GC development community for COTS products used to deliver part (or all) of a DCE service offering.

Rationale:

Many Departmental business and program applications are integrated with the desktop operating system and its layered products. In addition, many have integration points with foundational services such as Directory or Security.

Implications:

GC development standards and guidelines need to be established.

4.3.8 DCE PRINCIPLE 8: SERVICE ACCESSIBILITY BASED ON NETWORK SECURITY ZONE

There will be several security zones defined in the context of the Network Access Layer. These zones range from the public Internet to an Intranet to a secure network. These will be integrated with the directory-enabled GC network (several years out) and will define which DCE Services are available in which zone. For example, Messaging might be available in the public Internet zone, assuming the user is authenticated; however an internal financial application would not.

Rationale:

The capability of tailoring service accessibility based on network security zone provides for great flexibility and mobility for clients of the shared services. It removes the dependency on the type of client access device being used and the link to a physical location.

Implications:

This ability requires a common network infrastructure across the GC. Further it requires said network to be directory enabled such that devices, as well as users, are authenticated.

Access to applications and the execution thereof must be engineered such that they do not leave a footprint on the device they are being executed from. This may require an integrated terminal services solution “behind the wall”.

4.3.9 DCE PRINCIPLE 9: UTILIZE COTS PRODUCTS

DCE services will use Commercial Off-The-Shelf (COTS) products where possible.

Rationale:

The use of COTS software will lower cost through cost avoidance in developing and maintaining custom applications. Fewer custom applications will also enable lower TCO.

Implications:

Application functionality may be reduced in some cases by basing solutions on COTS rather than custom developed solutions. A cost benefit analysis will be performed when this scenario arises.

Establishing a discipline accepted by clients in which development decisions are based on ROI and TCO rather than needs and desires of clients.

Some Departments have significant investments in custom developed applications that are used in their current DCE delivery stack. These investments may be lost.

4.3.10 DCE PRINCIPLE 10: ESTABLISH A CROSS FUNCTIONAL CERTIFICATION FACILITY

Given that the ITSSO is not responsible for Departmental business or program applications, there needs to be rigorous ITSM processes established. As part of these processes, there needs to be a facility – or interface – which is responsible for certifying changes (and releases) such that infrastructure (ITSSO) changes don't adversely affect service/program delivery, and vice versa.

Rationale:

The service delivery chain (or stack) has many components combined and/or integrated to provide the client facing service offerings creating a dependency matrix that must be operational. A change to any one of these layers can adversely affect another. Formal certification (or QA) testing and acceptance must be performed before a change (or release) is implemented into production.

Implications:

The ITSM processes that are being developed for the ITSSO must clearly define this facility, its resources requirements and processes. This facility must provide for Departments to test their business/program application releases as well as infrastructure releases from the ITSSO.

During the due diligence phase of service negotiation, it would be beneficial for the ITSSO to understand how the respective Department performs this function today and may lead to an ability to adopt their solution.

4.3.11 DCE PRINCIPLE 11: MAINTAIN OR ENHANCE SERVICE DELIVERY PERFORMANCE

One of the primary considerations of client Departments when evaluating the adoption of shared services is that of service delivery performance, i.e. availability, accessibility, scalability and performance. Once rationalized between Departments, DCE services must be engineered to meet, or exceed, these delivery levels and balanced against the cost of delivery.

Rationale:

To facilitate adoption of shared services across the GC, it is imperative that the ITSSO maintain service delivery performance of existing Departmental DCE services.

Implications:

An assessment and rationalization of current Departmental service delivery performance metrics must be performed so that GC service level objectives can be defined. This process may assist in developing a tiered definition of service performance options.

APPENDIX A – REFERENCE DOCUMENTS

- Business Case for Enterprise IT Services – version 1.0 – November 8, 2004;
- Our Story, *ITS Transformation project overview on PWGSC Intranet*, http://source.pwgsc.gc.ca/direction/sit/text/transform_story-e.html, December 14, 2004
- Profile of GC IT Services – GC Enterprise Architecture – Profiles, CIOB – draft version 1.9, July 2005;
- Government Security Policy, http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp, February 1, 2002;
- Report of the Horizontal Review on Common Infrastructure and Service Delivery, draft version 21, December 11, 2003;
- Report on Common Infrastructure and Service Delivery – IT Infrastructure and Services Component, draft version 10, November 2003;
- Information Management / Information Technology Strategy and Roadmap, Agriculture and Agri-Food Canada, version 11.2, November 24, 2004;
- Service Management Improvement Program (SMIP) – Concept of Operations, version *x.x, date;*
- Business Continuity Strategy Design: How Far Apart Should Primary and Alternate Sites Be?, http://disaster-resource.com/newsletter/subpages/v96/meet_the_experts.htm, Disaster Resource Guide, August 10, 2005;
- Compass Task Force Report, Mandate IX – Identity and Access Management, draft version 2.02, August 5, 2005;
- Accessibility Domain Architecture, http://www.tbs-sct.gc.ca/fap-paf/documents/accessibility/access00_e.asp, Spring 2003; and
- Duty to Accommodate Persons with Disabilities in the Federal Public Service, http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/tb_852/ppaed_e.asp, June 3, 2002.

APPENDIX B – GLOSSARY OF ACRONYMS

AAC – Architecture Advisory Committee
CEO – Chief Executive Officer
CIOB – Chief Information Officer Branch
CoE – Centre of Excellence
COTS – Commercial Off-The-Shelf
DCC – Data Centre Consolidation Program
DCE – Distributed Computing Environment
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name Services
FAP – Federated Architecture Program
FINDS – Federated Infrastructure National Directory Service
GC – Government of Canada
HR – Human Resources
HVAC – Heating, Ventilation and Air Conditioning
IM – Information Management
IQTT – Identify, Qualify, Transfer and Transform process – also known as the "wave" approach to service adoption
IT – Information Technology
ITIL – Information Technology Infrastructure Library
ITSB – Information Technology Services Branch
ITSM – Information Technology Service Management
ITSSO – Information Technology Shared Services Organization
KPI – Key Performance Indicators
LAN – Local Area Network
LoB – Line of Business
MAN – Metro Area Network
MOU – Memorandum of Understanding
NOS – Network Operating System
OA – Office Automation
OS – Operating System
PDA – Personal Digital Assistant
PDF – Portable Document Format
PIM – Personal Information Manager
PKI – Public Key Infrastructure
PWGSC – Public Works and Government Services Canada
RFP – Request for Proposal
SAKMS – Secure Applications and Key Management Service (Internal GC Certificate Authority)
SAN – Storage Area Network
SDL – Service Delivery Locations
SLA – Service Level Agreement

SLO – Service Level Objective
SMIP – Service Management Improvement Program
SoR – Statement of Requirements
SRAS – Secure Remote Access Services
TBS – Treasury Board Secretariat
TISS – Technology and Internal Services Strategy
WAN – Wide Area Network