Canadian Heritage | Patrimoine canadien

AUDIT OF GOVERNMENT ON-LINE

FINAL REPORT

MAY 28, 2003

ASSURANCE SERVICES
CORPORATE REVIEW BRANCH
DEPARTMENT OF CANADIAN HERITAGE

Canada

Canadian Heritage | Patrimoine canadien

Canada

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....i

1.0 INTRODUCTION 1
1.1 Objectives 1
1.2 Scope 1

2.0 BACKGROUND 3
2.1 The Internet and Governments Globally 3
2.2 The Internet, the Government of Canada and the Department 3

3.0 STRENGTHS 6
3.1 A-Base Funding Secured for E-Services 6
3.2 Success of CCI and CHIN 6
3.3 Coordination Efforts Starting within the Department 6
3.4 Project Management Processes 7

4.0 AUDIT CONCLUSION AND OBSERVATIONS 8
4.1 Audit Conclusion 8
4.2 Audit Conclusion in Context 8
4.3 Governance 9
4.4 Annual and Long Term Planning 12
4.5 Management of Departmental GOL Investments 15
4.6 Information Architecture 17
4.7 Communications 19
4.8 Pre-project Approval Planning 21
4.9 Security 23

5.0 GOL RISKS 26

APPENDICES

Appendix A - Detailed CobiT Audit Criteria
Appendix B - Hierarchy of Cobit Domains
Appendix C - List of Criteria Evaluated

EXECUTIVE SUMMARY

On April 17, 2002 the Audit and Evaluation Committee of the Department approved the conduct of a Government On-Line (GOL) audit as part of the 2002-2003 internal audit plan. The objectives of the audit were two fold:

- to assess the appropriateness of the current management control framework for departmental GOL activities; and,
- to identify the key management risks to obtaining departmental GOL and Internet related objectives by 2005.

Based on the audit findings presented in the following pages, the audit team concluded that gaps exist in the current management control framework being used by the Department to bring its services on-line and meet the federal government GOL objectives by 2005. The majority of the gaps and recommendations for improvement are in the area of planning and organization, specifically: the GOL governance structure, annual and long-term planning, the management of departmental GOL investments, GOL related communications, and the departmental information architecture. Additionally, there is a need to improve management practices regarding pre-project approval planning activities and IT security. Additionally, it was noted that since the Department is only currently defining its GOL priorities, the department is at risk of not bringing its key services on-line by the 2005 target date.

In general, while this audit makes numerous recommendations for improvement, the audit team observed that the Department is moving in a positive direction. Specifically, in a majority of the key findings the audit team observed that the Department has been taking preliminary steps to address inadequacies in existing management practices and controls. However, more work is still required to bring the GOL management control framework to a state where senior management will be able to place a high degree of confidence in its effectiveness.

The following is a high level outline of the departmental strengths and audit findings that support this conclusion.

Findings

- **Governance:** The Department has not had a stable and clearly defined governance structure for GOL activities over the past four years. There is a risk that continued instability in the GOL governance framework will encourage

individual sectors to develop their own GOL priorities and projects without regard for the broader departmental GOL objectives.

- **Annual and Long-term Planning:** Elements of long and short term planning for GOL activities are happening within the Department, but a process does not exist to coordinate and align the disparate planning activities into a single, departmental GOL plan that includes long term plans, operational plans and short-term goals. There is a risk that GOL planning activities will continue to be uncoordinated between branches and sectors and not aligned to contribute to the recently approved departmental GOL vision and priorities.

- **Management of Departmental GOL Investments:** A process does not exist to ensure that the Department is fully leveraging its GOL related investments. There is risk that the lack of centralized oversight of IT and GOL spending will lead to duplication and that the Department may miss opportunities to increased efficiencies through leveraging existing resources.

- **Information Architecture**: The Department has not implemented an information architecture framework to enable efficient and effective collaboration with other departments and agencies. There is a risk that the current state of information architecture planning and standards will limit the Department's ability to move through the TBS GOL Service Completion Model, to efficiently and effectively transact with its clients, and collaborate with other government departments and agencies.

- **Communications:** A lack of awareness and understanding exists among staff and management regarding the Department's GOL vision, priorities, and organizational roles and responsibilities. There is a risk that the services offered by E-Services and KITS will not be effectively leveraged by staff and management due to a lack of awareness of the services offered and respective roles and responsibilities.

- **Pre-project Approval Planning**: The Department does not consistently undertake pre-project approval planning activities for IT and GOL projects. The lack of detailed pre-project analysis significantly increases the risk of project failures, as defined by escalations in original cost estimates, reductions in the quality and functionality of the final product delivered, and extensions in the original project timetables.

- **Security:** The Department has implemented a number of IT security controls but remains vulnerable to deploying Internet applications that have significant security flaws. There is a risk that a sector will develop an Internet application that is not secure and consequently, the Department will suffer loss of public

reputation and incur additional cost correcting the security issues.

Strengths

- **A-Base Funding Secured for E-Services**: Through the provision of stable funding the Department has provided the management of E-Services with increased certainty to allow for long-term planning. Stable funding should also enable E-Services management to focus more of its resources on delivering on its commitments rather than annual efforts to secure funding.

- **Success of CCI and CHIN**: The Department has two Special Operating Agencies that have developed extensive GOL/Internet experience and expertise: the Canadian Cultural Institute and the Canadian Heritage Information Network. CCI recently won a gold medal at the 2002 Government Technology Exhibition for "Unique Achievement in E-Government" for its Preserving My Heritage site

- **Coordination Efforts Starting within the Department**: The various sectors and branches involved in GOL are beginning to leverage their respective skills and experience. For example E-Services is starting to leverage the skills and experience of the Special Operating Agencies with advanced GOL/Internet knowledge and capacity and KITS and E-Services are starting to coordinate their activities and cooperate on GOL projects.

- **Project Management Processes**: The department has developed a detailed IT project process map that includes key activities, control/approval points, and deliverables.

1.0 INTRODUCTION

The requirement to conduct this audit was identified through the conduct of a department-wide program and corporate activity risk assessment and was included in the 2002-2003 Department of Canadian Heritage (PCH) Internal Audit Plan. Audit activities were conducted from October 2002 through February 2003 and included workshops and interviews with departmental staff and management drawn from all sectors, the conduct of an extensive documentation review, and a detailed analysis of findings. The audit program was based on two internationally recognized management control frameworks: Governance, Control and Audit for Information and Related Technology (CobiT), developed by the Information Systems Audit and Control Foundation; and, Criteria for Control Objectives (CoCo), developed by the Canadian Institute of Chartered Accountants.

1.1 Objectives

The objectives of this audit were two-fold:

- To assess the appropriateness of the current management control framework for departmental GOL activities; and,

- To identify the key management risks to obtaining departmental GOL and Internet related objectives by 2005.

1.2 Scope

The audit focused primarily on the management practices and processes of E-Services, Knowledge & Information Technology Services, the Canadian Conservation Institute; and the Canadian Heritage Information Network (CHIN). Established in 1972 as Special Operating Agencies, both CCI and CHIN are currently situated within the Heritage Branch of the Citizenship and Heritage Sector and are integrated into the Department's organizational structure and management practices.

By including the SOAs in the scope of this audit senior departmental management will be presented with a comprehensive assessment of the GOL management control framework and key risks to achieving its GOL objectives.

For the purposes of this audit GOL was defined to include not only those projects funded by Treasury Board Secretariat (TBS) through the GOL funding mechanism but also those projects and activities whose objective it is/was to offer departmental information and/or services through the Internet. As such, the GOL management control framework includes the policies, processes, and practices that combined, govern the Department's response and plan to meet the federal government GOL objectives for

2005.

Specific departmental GOL initiatives include: the Gateway (Culture.ca), the Cultural Observatory, the Cluster (CultureCanada.gc.ca), the corporate PCH website, and the Government of Canada Consultation Portal.

The audit did not include the activities of Portfolio agencies, as follows.

- Canada Council for the Arts
- Canada Science and Technology Museum Corporation
- Canadian Broadcasting Corporation
- Canadian Museum of Civilization
- Canadian Museum of Nature
- Canadian Race Relations Foundation
- Canadian Radio-television and Telecommunications Commission
- National Archives of Canada
- National Arts Centre
- National Battlefields Commission
- National Capital Commission
- National Film Board of Canada
- National Gallery of Canada
- National Library of Canada
- Parks Canada
- Status of Women Canada
- Telefilm Canada

2.0 BACKGROUND

2.1 The Internet and Governments Globally

The Internet and the new ways of working that it makes possible are both an opportunity and a challenge for both the public and private sectors around the world. The opportunity is to radically improve the quality and accessibility of public services, while at the same time reducing costs. Additionally, much higher levels of client service are possible, which can lead to much greater levels of client satisfaction. The challenge posed by the Internet is that if Governments do not adopt the new ways of working, public services will fall increasingly below the expectations of citizens, as they experience the benefits of the new technology in their transactions with the private sector.

The Internet is also a new communication and delivery channel that Government can use to reach out to its citizens to offer unprecedented levels of customer service, accessibility and horizontality, and a much more proactive approach to service delivery. Governments around the world are embracing service delivery improvement through the adoption of leading edge and emerging technologies.

- In 1999, the Canadian federal government signalled its commitment to e-government through the Throne Speech.
- In 2000, the Government of Ontario stated its goal to "Increase Ontarians' satisfaction with government services by becoming a world leader at delivering services on-line"
- Governments throughout Europe have set a target for all citizen transactions to be capable of being conducted electronically by around 2005.

It is within this environment that the federal government has embarked on its ambitious Government On-Line (GOL) initiative and subsequently that the Department has responded with the creation of the E-Services Branch.

2.2 The Internet, the Government of Canada and the Department

In 1999, the federal government undertook the commitment to enable Canadians to access all government information and services on-line at the time and place of their choosing by 2004. This vision has subsequently undergone several iterations.

- The 2001 federal budget allocated $600 million to implement the GOL strategy, extended the target date from 2004 to 2005, and changed the definition of what services to bring on-line from "all services" to "key services".

In response to the government-wide GOL initiative, PCH assigned responsibility for

planning and undertaking GOL and on-line projects between New Media Content and Government On-Line, Communications, Canadian Conservation Institute; and the Canadian Heritage Information Network. In the spring of 2002, this decentralized approach was replaced by a more centralized approach with the creation of E-Services Branch. Created in part to provide a focal point for all departmental Internet activities, E-Services vision, as identified in its Utility Model, is to advance PCH's on-line initiatives by promoting cultural participation and civic engagement, connecting and interacting with citizens, enhancing public access and fostering public dialogue, and by improving delivery of the Department's programs to citizens.

The table on the following page identifies that PCH received just over $2.4 million of the $600 million TBS GOL fund. It should be noted that the Common Front End initiative was part of a Pathfinder project to develop the client-facing front-end infrastructure for the Grants and Contributions Information Management System (GCIMS).

Project	$/Budget
PCH website	***2002-2003*** $165K - DGCOM $164K - CCOP $145K - A-Base
Canadian Cultural Observatory	***2001-2002*** $1.6M - CCOP (a portion of these funds were allocated to managing the GOL office) ***2002-2003*** $1.5M - CCOP $195K - A-Base
Gateway	***2001-2002*** $5.9M - CCOP ***2002-2003*** $6.8M - CCOP
Cluster	***2001-2002 (start-up)*** $400K - TBS $122.5K - Partners $120K - PCH ***2002-2003*** $55K - DGCOM $40K - TBS $220K - CCOP

Project	$/Budget
CHIN/Virtual Museum of Canada	***2001-2002*** $7M - CCOP ***2002-2003*** $7.5M - CCOP
CCI and preservation.gc.ca	***2001-2002*** $125K - PCH $35K - CCI ***2002-2003*** $75K - CCI
e-Dialogue(Consultation Portal, Meeting Place, Digital Commons, e-Consultation)	***2002-2003 (start-up)*** $200K - TBS (for the Consultation Portal) $400K - CCOP $90K - A-Base
Common Front End	***2001-2002*** $1.8M - TBS

3.0 STRENGTHS

This section of the report addresses the strengths of the current GOL Management Control Framework observed by the audit team.

3.1 A-Base Funding Secured for E-Services

- Through the Utility Model planning process, the Department has provided E-Services with stable A-Base funding for its core activities. Prior to this process, E-Services had funded its operations through a variety of departmental and central agency sources including: departmental A-Base funds, TBS, Canadian Culture Online Program (CCOP), and Communications. Through the provision of stable funding the Department has provided the management of E-Services with increased certainty to allow for long-term planning. Stable funding should also enable E-Services management to focus more of its resources on delivering on its commitments rather than annual efforts to secure funding.

3.2 Success of CCI and CHIN

- The Department has two Special Operating Agencies that have developed extensive GOL/Internet experience and expertise: the Canadian Cultural Institute and the Canadian Heritage Information Network. Both CCI and CHIN have been recognized for their excellence.

- **CCI:** CCI won a gold medal at the 2002 Government Technology Exhibition (GTEC) for "Unique Achievement in E-Government" for its Preserving My Heritage site. CCI is also actively pursuing the possibility of implementing new functionality to its website, including e-commerce and client/customer profiles.

- **CHIN:** CHIN has adopted effective Internet related management practices. Specifically, it includes a data integrity clause in its contracts with content providers for the Virtual Museum; it has implemented a metadata tool for its website; and, it uses on-going consultations to evaluate the effectiveness of its Internet Services.

3.3 Coordination Efforts Starting within the Department

- E-Services is starting to leverage the skills and experience of the SOAs with advanced GOL/Internet knowledge and capacity. For example, E-Services has recently signed an agreement with CHIN to assist with the marketing of the Gateway.

- KITS and E-Services are starting to coordinate their activities and cooperate on

GOL projects. For example, KITS has seconded a Director to E-Services to assist in the development on-line activities.

- The KITS Project Management Office has recently started providing project management advice to E-Services regarding project documentation processes.

3.4 Project Management Processes

- CHIN project management processes are documented and training has been developed for project managers. CHIN has recently trained 32 staff members through its own program.

- The KITS Project Management Office Project Management Process is a detailed IT project process map that includes key activities, control/approval points, and deliverables. Additionally, a standard Project Initiation Document (PID) has been created for use by all IT projects to attain project approval. Completion of this document requires the conduct of the following analysis: business analysis (including strategic alignment to PCH objectives, description of requirements, and benefit identification), technical analysis (including the presentation of different technical solutions) and cost estimates.

4.0 AUDIT CONCLUSION AND OBSERVATIONS

4.1 Audit Conclusion

Based on the audit findings we can conclude that gaps exist in the current management control framework being used by the Department to bring its services on-line and meet the federal government GOL objectives by 2005.

4.2 Audit Conclusion in Context

Following the structure of the CobiT Management Control Framework, the audit team assessed the Department's management practices, as they relate to GOL, in the following three broad categories: Planning and Organization; Acquisition and Implementation; Delivery and Support.

The majority of improvements recommended are in the area of Planning and Organization, specifically: the GOL governance structure, annual and long-term planning, the management of departmental GOL investments, GOL related communications, and the departmental information architecture. Additionally, there is a need to improve management practices regarding pre-project approval planning activities (Acquisition and Implementation) and IT security (Delivery and Support).

The following table outlines key gaps in the current management control framework.

Category	Management Practice	Current State
Planning and Organization	Governance	The Department has not had a stable and clearly defined governance structure for GOL activities over the past four years.
	Annual and Long-term Planning	Elements of long and short term planning for GOL activities are happening within the Department but a process does not exist to coordinate and align the disparate planning activities into a single, departmental GOL plan that includes long term plans, operational plans and short-term goals.
	Management of Departmental GOL Investments	A process does not exist to ensure that the Department is fully leveraging its GOL related investments in technology and training.

Category	Management Practice	Current State
	Information Architecture	The Department has not implemented an information architecture framework to enable efficient and effective collaboration with other departments and agencies.
	Communications	A lack of awareness and understanding exists among staff and management regarding the Department's GOL vision, priorities, and organizational roles and responsibilities.
Acquisition and Implementation	Pre-project Approval Planning	The Department does not consistently undertake pre-project approval planning activities for IT and GOL projects.
Delivery and Support	Security	The Department has implemented a number of IT security controls but remains vulnerable to deploying Internet applications that have significant security flaws.

4.3 Governance

4.3.1 Condition

The Department has not had a stable and clearly defined governance structure for GOL activities over the past four years.

4.3.2 Criteria

Define the enabling organisation and relationships.

4.3.3 Cause

The governance structure (including organizational roles and responsibilities) for GOL and planning for on-line projects has undergone three significant iterations since the GOL initiative was first announced in the 1999 federal Speech From The Throne.

The following is an outline of the evolution of the departmental GOL governance framework.

- **Prior to April 2002**: The early governance framework for GOL and on-line

activities primarily revolved around two management committees: the GOL Management Board and the GOL Task Team. The GOL Management Board was an Assistant Deputy Minister level committee with a mandate to set overall departmental GOL direction and approve GOL priorities. The GOL Task Team was a diagonal committee (all levels including DG) primarily tasked with GOL planning responsibilities. While the governance structure was clear during this period, there is little evidence that it functioned as intended. By the spring of 2002, the GOL Task Team had yet to finalize the development of a comprehensive inventory of PCH services. Additionally, the GOL Management Board did not perform the coordinating, monitoring and approval role outlined in its Terms of Reference.

Organizationally, responsibility for undertaking GOL and on-line projects was divided between a number of separate organizations, as follows: New Media Content and Government On-Line; Communications; CCI; and CHIN.

- **April to Fall 2002:** In the spring of 2002 the Department undertook a significant organizational restructuring. Through this process the Department moved to a structure that brought most GOL related activities into one organization, under one accountability, through the creation of the E-Services Branch.

  While organizational roles and responsibilities were becoming more streamlined and consolidated as a consequence of the reorganization, the reorganization negatively affected the GOL governance framework. Specifically all departmental management committees, with the exception of the Executive Committee, were suspended in the late spring of 2002. The Executive Committee did not assume the mandate and responsibilities of the GOL Management Board; and therefore, uncertainty developed within the Department regarding what executive level body was responsible for approving the GOL Task Team's planning activities and for providing GOL specific leadership regarding departmental GOL priorities, direction, and cross-sector coordination.

- **Fall 2002:** Since of the fall of 2002, a new departmental governance framework has been evolving. The evolving framework is constituted of three decision-making bodies: Executive Committee, Departmental Issues Management Committee, and IM/IT Strategy and Investment Committee. The principal working level of the new framework is the IM/IT Strategy and Investment Committee. While the mandate and role of the Committee has not been documented or approved by Executive Committee, it is the auditors' understanding that the intent of the new committee is to prioritize and approve new corporate IT investments. However, it is unclear what role this committee with play regarding GOL projects that are not identified as corporate in nature.

In addition to the above, two other GOL governance structures currently exist within the Department.

- **Gateway Project:** Apart from CHIN, the Gateway project represents the single largest departmental investment in GOL and Internet related projects, with approximately $6.8M spent in fiscal year 2002-2003. A National Advisory Board of fourteen prominent Canadians governs the Gateway project. The mandate of the Board is to advise the Minister of Canadian Heritage on: the general direction and continued evolution of the Program in light of the evolution of the Internet; the needs of users; the development of partnerships and tools to facilitate the creation and use of content; and the identification of priorities for investing in content.

- **CHIN and CCI**: Historically, both CHIN and CCI have not participated in the departmental GOL governance structure. Specifically, both CHIN and CCI have developed extensive websites without approval from the GOL Management Board.

4.3.4 Impact

There is a risk that continued instability in the GOL governance framework will encourage individual sectors to develop their own GOL priorities and projects without regard for the broader departmental GOL objectives.

4.3.5 Recommendation

It is recommended that the Director General of E-Services develop a governance structure (including the definition of organizational roles and responsibilities and oversight/approval structures) for consideration and approval by Executive Committee. Consideration should be given to including linkages to the Gateway project and the SOAs.

4.3.5 Management Response

The proposed governance structure was recommended and approved by DIMC on April 28 as part of the Service Delivery/GOL Strategy:

a) The current Committee structure i.e. Executive Committee, DIMC and DG Forum continue as the oversight/approval structure; the Executive Committee is the final approval body, while DIMC and the DG Forum oversee the initiatives and put forward for approval;

b) The IM/IT Strategy and Investment Committee had from the time of its inception a Draft Terms of Reference that described the

Committee's proposed role and mandate. This document is currently being revised to redefine the mandate and membership of the IM/IT Investment Strategy Committee to be responsible at the DG level for Service Improvement, GOL and IM/IT. All GOL activity would be required the endorsement of this committee prior to moving forward in the department. The intent is to seek formal approval by the Executive Committee of the IM/IT Strategy and Investment Committee within the PCH governance framework. The target for presentation of this revised mandate is June 2003.

c) Redefine the mandate and membership of the GOL Task Team to focus on Service Improvement, including GOL, at the working level. The target for presentation of this revised mandate is June 2003.

The mandate and definition of roles and responsibilities of each of these committee structures will be developed by each of the organizing bodies for approval by the Executive Committee.

Minutes of these committees will be recorded and posted to the departmental website.

4.4 Annual and Long Term Planning

4.4.1 Condition

Elements of long and short term planning for GOL activities are happening within the Department, but a process does not exist to coordinate and align the disparate planning activities into a single, departmental GOL plan that includes long term plans, operational plans and short-term goals.

4.4.2 Criteria

Define and develop a strategic plan.

4.4.3 Cause

The audit observed that long term and annual planning is happening at numerous levels within the Department. However, the planning activities do not contribute to a single, departmental GOL strategic plan and vary in detail and scope. Specifically, the audit team observed planning activities at the departmental level, within E-Services, and SOAs.

Department Planning: It is our understanding that PCH does not have a recent history of integrating the different planning activities of each sector into an integrated long and short-term departmental plan. However, in the fall of 2002, Executive Committee approved an initiative from Corporate Planning and Management Branch to implement an Integrated Planning and Reporting Framework for the Department. Phase one of the plan is currently underway, it is anticipated that a review of the model will be completed at the end of this fiscal year (2002-2003).

- Regarding long and short term planning for GOL at a departmental level, recent progress has been made to identify a GOL vision for PCH. In a presentation to the Departmental Issues Management Committee (November 2002), a revised version of PCH's GOL vision was presented and approved. Additionally, PCH's four key service areas were also presented and approved. Planning activities at the departmental level that remain to be completed include: validating the GOL vision; translating the GOL vision into clear objectives that can be used by the sectors and branches in their annual planning activities; and completing short and long-term strategies for GOL within PCH.

- **E-Services:** Since its creation in April 2002, E-Services has primarily focused on developing its organization; conducting individual project planning activities; and securing A-Base funding. As such, integrated long and short-term planning activities are only now being conducted. In December 2002, E-Services presented a Utility Model to Executive Committee that identified GOL investment opportunities and its approach to responding to the Department's 2002-2003 Report on Plans and Priorities commitment of "harnessing modern technology will be a key strategy for communicating with Canadians". While the Utility Model is not a strategic or annual planning document, it does lay the foundation for the Branch's long-term plan by outlining where it requires A-Base funding and the resources required to support its programs. The approval of the Utility Model was a key milestone in the Branch's efforts to plan for future activities.

- **CHIN & CCI:** Historically, CHIN and CCI have not been included in departmental GOL planning activities, even though they are the most advanced in their delivery of services on-line. However, CHIN and CCI have developed their own strategic plans. The Canadian Conservation Institute for example, has a business plan that targets what it wants to achieve over the next three years, including the direction of its on-line initiatives.

4.4.4 Impact

There is a risk that GOL planning activities will continue to be uncoordinated between branches and sectors and not aligned to contribute to the recently approved departmental GOL vision and priorities.

4.4.5 Recommendation

It is recommended that the Director General of E-Services, with input from the Chief Information Officer (CIO), develop a Departmental GOL strategic plan for approval by Executive Committee. The process of developing the GOL strategic plan should be integrated into the new Integrated Planning and Reporting Framework and be linked to the priorities and objectives outlined in the PCH 2003-2006 Business Plan.

4.4.5 Management Response

It should be noted that the departmental Integrated Planning and Reporting Framework is still in early stages of development. As this framework and related processes mature within the department, E-Service will ensure that it keeps step with the progression. The IM/IT Strategic Investment Committee will discuss all projects, including those for GOL. It is estimated that it will take a full 2-year cycle before we reach a fully integrated planning process in the department. GOL Strategic Planning will be integrated into the 2004 - 2005 planning cycle.

While both E-Services and KITS have recently secured Utility/A-Base funding, additional effort and coordination is required to ensure that the A-Base post-delivery operations impacts of new investments are identified and appropriately costed and that additional funds are actually provided to the relevant organizations after implementation and that an assessment of projected versus actual costs is undertaken after a sufficient operational interval has passed. The presentation of a Business Case identifying funding implications will be made in the first quarter of 2004.

A long term GOL strategy must also be linked directly with the Service Strategy and the IM/IT Strategy, as all GOL projects will have implications on service delivery as well as IM and IT. The inventory report, which was completed by the GOL Task Team in the fall of 2002, can be used as a starting point for the development of a long term GOL strategy. The client satisfaction surveys, which will be undertaken in pilot sites under the Service Improvement initiative, will also provide valuable information towards the development of the long term GOL strategy in the department. The Service Delivery/GOL Strategy approved by DIMC on April 28, 2003, committed to the presentation of a Business Case to Executive Committee by March 30, 2004.

4.5 Management of Departmental GOL Investments

4.5.1 Condition

A process does not exist to ensure that the Department is fully leveraging its GOL related investments.

4.5.2 Criteria

Managing the investment.

4.5.3 Cause

Currently, there is no centralized process/control to review, assess and coordinate all Departmental IT and related spending. Funding decisions regarding IT and GOL related projects are made at the sector and branch level without a formal mechanism to assess whether all departmental investments are being fully leveraged, or to prevent the duplication of spending.

Audit findings indicate that in the past PCH has not maintained an investment strategy for Internet-related activities. The Department is evolving, however, and is in the process of implementing limited controls over IT spending. Recently an IM/IT Strategy and Investment Committee, led by the CIO, was created. To date, the mandate, scope, and responsibilities of the Committee have not been documented nor communicated. However, it is the auditors understanding the Committee will coordinate, prioritize and recommend, to Executive Committee, IT projects that benefit the department as a whole. It is not clear at this time whether the Committee will review and monitor projects funded through a sector's A-Base funding.

The audit team observed that potential duplication or lack of coordination exists in the areas of technology and training, as follows.

Technology: As discussed above, control over IT spending that originates within a sector and uses A-Base funds is a potential area of concern. Specifically, a risk exists that projects will be developed with technology that is not supported by KITS or that does not leverage existing platforms and/or information resources. The following is one example of this risk.

The GCIMS project was led and developed by a team in Winnipeg with little input and coordination of KITS. The system was developed using a Microsoft Sequel Server database rather than an Oracle database, which is used for the Department's SAP and PeopleSoft applications. Using a Microsoft Sequel Server does not leverage the existing Oracle knowledge and experience in KITS.

Training: There is a duplication of project management processes and practices within the Department as CHIN and KITS follow different project management methodologies. CHIN recently developed its own project management course without the input of the KITS Project Management Office and is now offering training to its staff. Approximately 32 employees (at $700 per person) attended a three-day session conducted by external trainers. Duplication exists as the KITS Project Management Office has developed a set of different tools and uses a different project management methodology for similar projects.

4.5.4 Impact

There is risk that the lack of centralized oversight of IT and GOL spending will lead to duplication and that the Department may miss opportunities to increased efficiencies through leveraging existing resources.

4.5.4 Recommendation

It is recommended that, based on advice provided by the CIO, the Executive Committee approve a process to ensure that the Department is fully leveraging its IT and related investments.

4.5.4 Management Response

IT investments will be incorporated into sector business plans during 2004/05 and as such will be reviewed by senior level committees as part of the business planning exercise.

As of FY 2003/04, the IT Investment Committee will review IT investments from a departmental perspective.

While the report notes that there are two project methodologies in place within PCH, the consistency, timing and quality of the implementation and adherence to the methodologies should be an area of concern. KITS continues to place emphasis on Quality Assurance/Quality Control for Project Management practices/procedures in order to ensure that projects are well managed.

4.6 Information Architecture

4.6.1 Condition

The Department has not implemented an information architecture framework to enable efficient and effective collaboration with other departments and agencies.

4.6.2 Criteria

Define the Information Architecture.

4.6.3 Cause

Planning Activities: The development and implementation of Department-wide information architecture and enterprise architecture principles and standards are in the early phases of being addressed. Within the last two years, an Architecture and Standards unit was created within IM/IT Planning, Policy and Performance of KITS. The unit is staffed by a Deputy Director and 2 FTE's and has initiated the development of the foundational planning components required for information architecture. Specifically, in December of 2002 the unit released the fourth version of the "PCH Enterprise Architecture: Architecture Principles, Best Practices, Domain Team Structure, Development Strategy, & Glossary Of Terms" document.

Current Standards & Practices: While initial enterprise and information architecture planning activities are underway within the Department, significant gaps exist in current practices and standards. Specifically, evidence was not collected that PCH is planning to:

- Conduct a detailed analysis of its current information architecture or develop a target information architecture for the desired future state. This activity is required for effective and efficient Department-wide management of its information holdings.

- Map its data holdings to fully understand and document what data it maintains and where it resides. Specifically, the Department has not undertaken a process nor does it have a regular process to identify and document the data elements that it maintains in its information systems.

The Chief Information Officer Branch of TBS has defined that the GOL end state for 2005 will include the provision of "horizontal services" and "joined-up services" to Canadian citizens. This vision anticipates that departments and agencies will work collaboratively to offer services to citizens in a client centric presentation rather than the traditional approach that has emphasised departmental divisions of responsibility.

Additionally, the TBS GOL Service Completion Model assesses the level of service integration with other government departments and services. For collaboration to occur, all parties to a collaboration require a basic understanding of their information holdings and architecture.

The audit team anticipates that additional pressure for information architecture planning will arise over the next year as PCH starts bringing current GOL projects on-line. Specifically, the Department is planning to launch the Gateway and the Cultural Observatory this year. Additionally, the Department is currently hosting and or managing numerous other websites including: CultureCanada.gc.ca, the PCH Internet site, the PCH Intranet site, the PCH HR site, The Virtual Museum, CHIN, and Preserving My Heritage. For the Department to effectively leverage the content from each of these sites, additional information architecture planning will be required.

An example of inefficient information architecture was observed in the CFE project. Specifically, the pilot solution captures and stores client contact information in its own separate database. Similar information is also captured and stored in the Department's SAP application. Should this pilot solution be adopted by PCH, standards and practices will be required to identify the authoritative source of this information.

4.6.4 Impact

There is a risk that the current state of information architecture planning and standards will limit the Department's ability to move through the TBS GOL Service Completion Model, to efficiently and effectively transact with its clients, and collaborate with other government departments and agencies.

4.6.5 Recommendation

It is recommended that the CIO develop an information architecture framework that will satisfy its internal information systems requirements and anticipated GOL requirements. Consideration should be given to incorporating this work into the current enterprise architecture planning activities.

4.6.5 Management Response

We agree with all the comments regarding the need for departmental information architecture. However while the COBIT Framework model only includes Information Architecture, KITS activities have been aligned with the Government of Canada/Government Online Federated Architecture Model which envisions an overall Enterprise Architecture that incorporates and integrates a hierarchy of Business, Information, Application and

Technology Sub-Architectures. In this context describing and defining the Business Architecture will be key in the development of PCH's Information Architecture. Plans to develop the current and target sub-architectures have been incorporated into the recently developed project pipeline for the implementation of the IM/IT Strategic Framework. This is a high priority item which has been submitted to the IT Investment Committee for funding during FY2003/04. The Committee will base its decision based on resources available and competing priorities.

4.7 Communications

4.7.1 Condition

A lack of awareness and understanding exists among staff and management regarding the Department's GOL vision, priorities, and organizational roles and responsibilities.

4.7.2 Criteria

Communicate management aims and direction.

4.7.3 Cause

The audit team consistently received comments from audit participants that indicate a lack of awareness and understanding of the Department's response to the federal government's GOL initiative and the internal division of roles and responsibilities for GOL. Specifically, the audit team observed that:

- One of the GOL Task Team's original objectives was to enhance GOL related communications. It was the responsibility of each individual team member to ensure that GOL communications were passed along to their individual sectors. However, the GOL Task Team has not held regularly scheduled meetings in 2002 and it is unclear how effective this form of communications has been in disseminating information throughout the sectors and branches.

- Internal communications throughout the Department regarding GOL roles and responsibilities has been limited. Interview participants generally did not have a clear understanding of the different roles and responsibilities of KITS and E-Service and the respective services offered by both organizations. Specifically, some ambiguity exists regarding which is the proper organization to approach first when planning for GOL projects.

- Information regarding the Department's GOL vision and priorities has not been

broadly communicated. Most interview participants identified the Gateway and Cultural Observatory as the Department's key GOL priorities.

4.7.4 Impact

There is a risk that the services offered by E-Services and KITS will not be effectively leveraged by staff and management due to a lack of awareness of the services offered and respective roles and responsibilities.

4.7.5 Recommendation

It is recommended that the Director General of E-Services develop and implement a communications strategy to raise the level of awareness among staff and management regarding GOL roles and responsibilities, vision, and priorities.

4.7.5 Management Response

A communications strategy was developed and approved in May 2002. Although it was never implemented, E-Services is currently working with the Communications Branch to update the strategy and to develop an implementation plan. The strategy will need to be broadened to ensure integration of Service Improvement, GOL and IM/IT. Also, as part of the original strategy, a multi-media presentation was developed and with minor adjustments will be ready to be released across the department. The revised Communications Strategy will be presented to the Governance groups by March 31, 2004.

Externally, the department currently reports annually to Treasury Board and has posted a GOL report to the Canada site for Canadians.

To assist in improving communications between E-Services and KITS there should be clearer documentation on agreed upon accountabilities, responsibilities and roles vis a vis the two organizations. This will be developed by March 31, 2004.

Additional efforts in both organizations to improve and regularize the communication, distribution and access to plans, updates, status reports, decisions etc. is necessary and would be extremely beneficial.

4.8 Pre-project Approval Planning

4.8.1 Condition

The Department does not consistently undertake pre-project approval planning activities for IT and GOL projects.

4.8.2 Criteria

Identify automated solutions and conduct pre-project approval planning activities.

4.8.3 Cause

Within the past three years, the Department has developed the required organizational and process infrastructure to support effective IT project management and specifically the conduct of pre-project approval feasibility and planning assessments.

- **Organizationally:** KITS has established the Project Management Office in the Client Partnerships and Strategic Investments group. This office is led by a manager, staffed with four project managers, and provides project management advice and support services to managers undertaking IT and related projects.

- **Procedurally:** The Project Management Office has developed a detailed IT project process map that includes key activities, control/approval points, and deliverables. In addition a standardized project planning template (Project Initiation Document) has been developed for use by all IT projects to attain project approval.

While the organizational and process infrastructure exists to support effective IT project management, the audit team observed that the Department does not consistently conduct detailed pre-project approval assessments and studies for all IT and GOL related projects. Examples of this were observed as follows.

- The **Gateway Project** has been in the planning and development phase for the past three years, represents a significant investment of departmental resources (over $12M in the last 2 years) and is scheduled for launch in March of this year. However, it is only within the last six months that this project has initiated work on developing a detailed business case for this project.

- The **CFE Project**, representing an investment of $1.8M, has been completed and delivered to TBS. However, the Department is only currently testing the application with its client base and developing a business case to assess its potential adoption and use by the Department.

The audit team also observed the following contributing factors to this condition.

- **Departmental Past Practices**: The majority of audit interviewees stated that the Department does not have a history of conducting detailed pre-project planning activities before undertaking IT-related projects. Specifically, interviewees stated that managers often skip planning activities in favour of trying to meet deadlines and finish projects early.

- **Decentralized IT Project Management Roles and Responsibilities**: The Department has not implemented controls to ensure that all IT projects undertaken within the Department comply with the KITS Project Management Office's Project Management Process. Currently, the Department follows a decentralized approach to project management where projects undertaken outside of KITS are not required to follow the KITS Project Management Office's Project Management Process nor are required to develop a Project Initiation Document. Additionally, project management responsibilities have been decentralized to individual project managers within the sectors.

4.8.4 Impact

The lack of detailed pre-project analysis significantly increases the risk of project failures, as defined by escalations in original cost estimates, reductions in the quality and functionality of the final product delivered, and extensions in the original project timetables.

4.8.5 Recommendation

It is recommended that the CIO develop a process to ensure that detailed pre-project approval planning activities/feasibility studies are conducted prior to approval of all IT and GOL-related projects.

4.8.5 Management Response

The PID or Project Initiation Document was originally intended to be a short one or two page document that would describe at a high level the purpose and scope of a proposed project. As such a governance body would review it and approval would then be given to begin the pre-project planning phase. Unfortunately over time the PID has evolved into the document which is prepared to obtain approval to begin actual implementation of a project. Consideration should be given to scaling back the PID to meet its original purpose with the majority of the content of the current PID being incorporated into a Project Approval

Document/Business Case.

Currently the IM/IT Strategy and Investment Committee is evolving the practice of developing a project pipeline whereby potential projects would be identified at a high level and then reviewed and approved with seed funding for the development of a business case and initial project plan/charter all of which would serve as a input and basis for consideration of full project approval and funding. This will be completed by March 2004.

4.9 Security

4.9.1 Condition

The Department has implemented a number of IT security controls but remains vulnerable to deploying Internet applications that have significant security flaws.

4.9.2 Criteria

Ensure systems security.

4.9.3 Cause

Over the past three years KITS has developed the required supporting infrastructure for effective IT security management within the Department. Specifically, KITS has taken the following steps.

- Hired a full-time IT Security Manager in November 1999.
- Conducted a Departmental Threat and Risk Assessment on the Department's network infrastructure and corporate systems.
- Developed an IT Security organization within KITS. Currently the organization is a sub-unit of IT Infrastructure Services and is responsible for managing the Department's firewall, infrastructure, and PKI applications.
- Developed a related policy framework, including:
  - IT Security Policy: Chapter 4 of the Departmental Security Policy;
  - Internet Appropriate Use Policy; and
  - E-mail Appropriate Use Policy.

However, the audit team observe a significant weakness in the existing practices. As previously stated in Section 4.8.3, the Department has not implemented controls to ensure that all IT projects undertaken within the Department comply with departmental IT standards. Specifically, IT projects funded by a sector's A-Base are not required to follow the KITS project management processes nor are they required to involve the KITS IT Security unit in the planning phases of the project. Without some form of

control to ensure IT security issues are addressed in the planning phase of IT projects, the Department increases the risk that systems will be developed that have significant security inadequacies.

It is important to note, however, that the Department does employ a detective control to mitigate the risk of an insecure application being placed in a live environment. (A detective control detects an error or problem after it has occurred while a preventative controls prevents a risk from occurring.) Specifically, all Internet applications are reviewed by IT Security before IT Infrastructure Services will connect the application to the PCH network. This is a detective control as it reviews applications at the end of the systems development life cycle and only after the majority of the IT investment has been spent. Additionally, IT Security does not have the authority to deny a request to place an application on-line. The following is a recent example of this weakness.

- The CFE was developed in Winnipeg without the early input of the IT Security group in Ottawa. When the development was complete, the project team requested a review from IT Security. The review identified significant security issues and recommended that it not be placed in a live environment. CFE was subsequently connected to the Internet without significant modification and was subject to a successful malicious attack within 24 hours of connection to the Internet.

In addition to the above, the current practice is contrary to the intent of the Government Security Policy (GSP). Specifically, Section 10.12 - Information Technology Security of the GSP states that, "Departments must ensure that Information Technology Security is an integral part of each stage in the system development life cycle. Security requirements and related funding must be identified and included in planning, requests for proposals, and tender documents for IT projects."

4.9.4 Impact

There is a risk that a sector will develop an Internet application that is not secure and consequently, the Department will suffer loss of public reputation and incur additional cost correcting the security issues.

(Please note, this finding addresses the application and management of security controls within the Department. Observations and comments from audit participants were not received that the Department's current data holdings are at risk. Rather, it was noted that the lack of preventative controls poses a future risk as the department brings more transactional applications on-line.)

4.9.5 Recommendation

It is recommended that the CIO develop a policy or procedure, for approval by Executive Committee, that will ensure all IT projects require input from IT Security prior the commencement of development activities.

4.9.5 Management Response

It should be noted that while KITS has a long established Change Management Committee, which is intended to ensure that potential issues and problems are identified before changes are made in the production environment, E-Services/GOL initiatives have not been submitted to the Committee for consideration.

KITS agrees with the need to consider Security issues early in the project planning lifecycle and to engineer in compliance and solutions at the beginning rather than trying to retrofit at the end of the project.

KITS has a well established process to ensure that departmental applications meet IT security standards. However, until there is a corporate governance policy, KITS provides advice only on sector applications and therefore cannot ensure that IT security standards are enforced on these applications. Senior management is looking into the corporate IT governance this year which would include security governance.

5.0 GOL RISKS

The following table outlines the risks, sources and consequences identified though the audit activities.

Risk Name		Risk Statement	Risk Source
1	**Governance Structure**	• There is a risk that continued instability in the GOL governance framework will encourage individual sectors to develop their own GOL priorities and projects without regard for the broader departmental GOL objectives.	• The GOL governance structure (including organizational roles and responsibilities) has undergone three significant iterations since the GOL initiative was first announced in the 1999 federal Speech From The Throne. • The current governance structure is evolving and the roles and responsibilities of the various committees and organizations are undocumented.
2	**Annual and Long Term Planning**	• There is a risk that GOL planning activities will continue to be uncoordinated between branches and sectors and not aligned to contribute to the recently approved departmental GOL vision and priorities.	• Long term and annual planning is happening at numerous levels within the Department. • Some planning activities are happing at the departmental level, within E-Services, and the SOAs • Planning activities do not contribute to a single, departmental GOL strategic plan and vary in detail and scope.
3	**Management of Departmental GOL Investments**	• There is risk that the lack of centralized oversight of IT and GOL spending will lead to duplication and that the Department may miss opportunities to increased efficiencies through leveraging existing resources.	• Funding decisions regarding IT and GOL related projects are made at the sector and branch level. • A formal mechanism to assess whether GOL investments are being fully leveraged, or to prevent the duplication of spending is not evident. • Currently, there is no centralized control over IT and related spending.

Risk Name		Risk Statement	Risk Source
4	**Information Architecture**	• There is a risk that the current state of information architecture planning and standards will limit the Department's ability to move through the TBS GOL Service Completion Model, to efficiently and effectively transact with its clients, and collaborate with other government departments and agencies.	• The development and implementation of Department wide information architecture and enterprise architecture principles and standards are in the early phases of being addressed. • A detailed analysis of PCH's current information architecture or target architecture has been conducted. • PCH has not mapped its data holdings to fully understand and document what data it maintains and where it resides. • Additional pressure for information architecture planning may arise over the next year as PCH starts bringing the current GOL projects on-line.
5	**Communications**	• There is a risk that the services offered by E-Services and KITS will not be effectively leveraged by staff and management due to a lack of awareness of the services offered and respective roles and responsibilities.	• Internal communications throughout the Department regarding GOL roles and responsibilities has been limited. • A lack of awareness exists among staff and management regarding which is the proper organization to approach first when planning for GOL projects (KITS or E-Services). • Information regarding the Department's GOL vision and priorities has not been broadly communicated.

Risk Name		Risk Statement	Risk Source
6	**Pre-project Approval Planning**	• The lack of detailed pre-project analysis significantly increases the risk of project failures, as defined by escalations in original cost estimates, reductions in the quality and functionality of the final product delivered, and extensions in the original project timetables.	• The Department does not have a history of consistently conducting detailed pre-project approval assessments and studies for all IT and GOL related projects. • The Department has not implemented controls to ensure that all IT projects undertaken within the Department comply with the PMO Project Management Process.
7	**Security**	• There is a risk that a sector will develop an Internet application that is not secure and consequently, the Department will suffer loss of public reputation and incur additional cost correcting the security issues.	• The Department has not implemented controls to ensure that all IT projects undertaken within the Department comply with departmental IT standards. • IT projects funded by a sector's A-Base are not required to follow the KITS project management processes nor are they required to involve the KITS IT Security unit in the planning phases of the project.

Appendix A
Detailed CobiT Audit Criteria

Section	Criteria	Detailed Control Objective
4.3 Governance	CobiT Criteria PO4: Define the Organisation and Relationships	Control over the process of defining the organisation and relationships that satisfies the business requirement to deliver the right services is enabled by an organization suitable in numbers and skills with roles and responsibilities defined and communicated, aligned with the business and that facilitates the strategy and provides for effective direction and adequate control.
4.4 Annual and Long Term Planning	CobiT Criteria PO1: Define a Strategic Plan	Control over the process of defining a strategic plan that satisfies the business requirement to strike an optimum balance of information technology opportunities and business requirements as well as ensuring its further accomplishment is enabled by a strategic planning process undertaken at regular intervals giving rise to long-term plans. The long term plans should periodically be translated into operational plans setting clear and concrete short-term goals.
4.5 Management of Departmental GOL Investments	CobiT Criteria PO5: Managing the Investment	Control over the process of managing the investment that satisfies the business requirement to ensure funding and to control disbursement of financial resources is enabled by a periodic investment and operational budget established and approved by the business.
4.6 Information Architecture	Cobit Criteria PO2: Define the Information Architecture	Control over the process of defining the information architecture that satisfies the business requirement of optimizing the organisation of the information systems is enabled by creating and maintaining a business information model and ensuring appropriate systems are defined to optimize the use of this information.

Section	Criteria	Detailed Control Objective
4.7 Communications	Cobit Criteria PO6 : Communicate Management Aims and Direction	Control over the process of communicating management aims and direction that satisfies the business requirement to ensure awareness and understanding of those aims is enabled by policies established and communicated.
4.8 Pre-project Approval Planning	Cobit Criteria AI1: Identify Automated Solutions	Control over the process of identifying automated solutions that satisfies the business requirement of ensuring an effective and efficient approach to satisfy the user requirements is enabled by an objective and clear identification and analysis of the alternative opportunities measured against user requirements.
4.9 Security	Cobit Criteria DS5: Ensure Systems Security	Control over the IT process of ensuring systems security that satisfies the business requirement to safeguard information against unauthorised use, disclosure or modification, damage or loss is enabled by logical access controls which ensure that access to systems, data and programmes is restricted to authorised users.

Appendix B
Hierarchy of Cobit Domains

Category	Orientation of Criteria	Impacts
Planning and Organization	• Focuses on management practices that are applied organization-wide. • Are the "foundational pieces" to an effective management control framework.	• Directly affect an organization's ability to meet its high-level goals and objectives.
Acquisition and Implementation	• Focuses on management practices that are applied at the project level. • Builds on effective planning and organization.	• Affect an organization's ability to achieve project successes.
Delivery and Support	• Focuses on management practices that are used to sustain projects after implementation. • Build on effective planning and organization, and acquisition and implementation.	• Affect an organization's ability to sustain project successes.

Appendix C
List of Criteria Evaluated

Domain	Process		Include
Planning and Organization	**P01**	Define a strategic Plan	Recommendation included in report
	P02	Define the information architecture	Recommendation included in report
	P03	Determine the technologic direction	Scoped out in planning phase
	P04	Define the organisation and relationships	Recommendation included in report
	P05	Manage the investment	Recommendation included in report
	P06	Communicate management aims and direction	Recommendation included in report
	P07	Manage human resources	Scoped out in planning phase
	P08	Ensure compliance with external requirements	Data gathered, recommendation not required/pursued.
	P09	Assess risks	Data gathered, recommendation not required/pursued.
	P010	Manage projects	Strength
	P011	Manage quality	Data gathered, recommendation not required/pursued.
Acquisition & Implementation	**AI1**	Identify automated solutions	Recommendation included in report.
	AI2	Acquire and maintain application software	Scoped out in planning phase
	AI3	Acquire and maintain technology infrastructure	Scoped out in planning phase

Domain	Process		Include
	AI4	Develop and maintain procedures	Scoped out in planning phase
	AI5	Install and accredit systems	Data gathered, recommendation not required/pursued.
	AI6	Manage changes	Data gathered, recommendation not required/pursued.

Domain	Process		Include
Delivery & Support	**DS1**	Define and manage service levels	Data gathered, recommendation not required/pursued.
	DS2	Manage third-party services	Data gathered, recommendation not required/pursued.
	DS3	Manage performance and capacity	Data gathered, recommendation not required/pursued.
	DS4	Ensure continuous service	Data gathered, recommendation not required/pursued
	DS5	Ensure system security	Recommendation included in report
	DS6	Identify and allocate costs	Scoped out in planning phase
	DS7	Educate and train users	Scoped out in planning phase
	DS8	Assist and advise customers	Data gathered, recommendation not required/pursued.
	DS9	Manage the configuration	Scoped out in planning phase
	DS10	Manage problems and incidents	Data gathered, recommendation not required/pursued.
	DS11	Manage data	Data gathered, recommendation not required/pursued.
	DS12	Manage facilities	Scoped out in planning phase
	DS13	Manage operations	Scoped out in planning phase

Domain	Process		Include
Monitoring	**M1**	Monitor the processes	Data gathered, recommendation not required/pursued.
	M2	Assess internal control adequacy	Scoped out in planning phase
	M3	Provide independent assurance	Data gathered, recommendation not required/pursued.
	M4	Provide for independent audit	Scoped out in planning phase