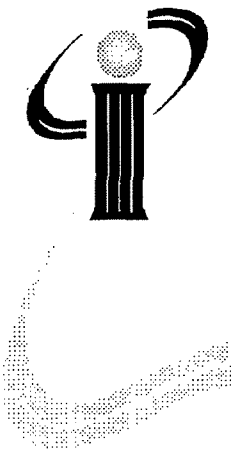

1999-715

Audit of the Use of Internet Technologies in the Business Process - Electronic Service Delivery

November 9, 1999

Public Works and Government Services Canada

Audit and Review

Travaux publics et Services gouvernementaux Canada

Vérification et Examen

Canada

Table of Contents

Executive Summary

Authority for the Project

This audit was approved by the Audit and Review Committee as part of the 1999/2000 Audit and Review Branch (ARB) Plan.

Objectives

To assess the adequacy of the Management Control Framework (MCF) around the Department's use of Internet technology in support of Public Works and Government Services Canada (PWGSC) programs and Government of Canada (GOC) initiatives.

Scope

The audit focused on the adequacy of the MCF related to the use of Internet technology to support Electronic Service Delivery (ESD) and other PWGSC business objectives (including support of GOC initiatives).

Approach

The approach used during this audit included a review of documentation and information in PWGSC paper-based files (including relevant prior audits) and various PWGSC and external Inter/Intranet sites. As well, interviews were conducted with numerous PWGSC managers representing the major PWGSC business lines, as well as with an official at the Treasury Board Secretariat (TBS).

Background

The Government of Canada has established a goal of making Canada the most connected nation in the world. Governments are to show leadership by acting as model users of technologies, serving to demonstrate the advantages of electronic Commerce (EC) and to build trust. Accordingly, Government use of EC is growing - EC is projected to grow rapidly and become the preferred means to conduct business. Although it can be defined narrowly or broadly, EC is generally seen as an Internet application.

The PWGSC Information Management Plan (IMP) 1998-2001 reflects PWGSC's increased interest in EC and ESD to fulfill business objectives. The IMP recognizes that the effectiveness of PWGSC's Automated Buyer Environment (ABE) rests on advancement of ABE connectivity

with client departments and suppliers. Similarly, the IMP notes the Government Operational Service (GOS) Branch has identified an electronic commerce initiative to expand electronic remittance, payment inquiries and payment issues. The IMP also notes Government Telecommunications and Informatics Services (GTIS) Branch plans to support common informatics services in the EC areas of electronic directories, infrastructure components, electronic security and Government Electronic Data Interchange Service (GEDIS).

PWGSC has been active on EC and ESD from both the external and internal perspectives. Externally, GTIS and the TBS began work in April 1999 on a centrally funded, procured and managed federated architecture supporting a secure GOC ESD channel. Internally, PWGSC is working on its Electronic Procurement and Settlement (EP&S) project to develop an integrated electronic end-to-end procurement through settlement process.

Key Findings

PWGSC's objectives for ESD using Internet technology are well defined and communicated, and consistent with those at the government-wide level. Similarly, PWGSC Branch ESD-related goals are consistent with and support the broader PWGSC objectives.

PWGSC has implemented various mechanisms to manage and coordinate ESD-related activities and initiatives with external stakeholders, including TBS, other government departments (OGDs), and the private sector. These mechanisms include the joint PWGSC/TBS work on the Federated Architecture, and the creation of the Strategic Services Sector (SSS) to support government departments in their program delivery and to explore partnership opportunities with the private sector.

PWGSC has also implemented mechanisms to improve coordination and communication among GTIS sectors, and with and among business branches. These include the establishment of the Architecture and Engineering Steering Committee (AESC) along with its supporting structure of Centres of Expertise (COEs) to evaluate business proposals for technical feasibility and appropriateness; the establishment of an infrastructure and processes to coordinate the creation of Inter/Intranet sites and to ensure information published on those sites adheres to federal government and departmental requirements; and the establishment of project teams to coordinate and deliver specific ESD components and products. As well, GTIS is also hosting one-day retreats with PWGSC business branches which supplement the already-established interface points between GTIS and the Business Branches. Finally, there is also a proposal to develop an Enterprise Project Office to help with the coordination of GTIS projects. However, as many of these elements are new, under review, or to be implemented, continued work is required to ensure that more effective communication and coordination are achieved.

Information Management / Information Technology (IM/IT) within PWGSC has been managed through a departmental governance framework which features a hierarchy of governance committees led by the Assistant Deputy Minister (ADM) level Information Management Committee (IMC) and a structured IM/IT governance process supplemented by similar frameworks at the branch level. However, this corporate IM/IT governance framework is

currently in a state of transition with new committees being identified (such as the AESC) and existing committees put on hold. This has resulted in a greater reliance on GTIS to ensure that horizontal/corporate activities and issues are brought forward to IMC. In order to stabilize PWGSC's IM/IT governance structures and processes, priority should be given to completing the review and renewal of the corporate IM/IT governance framework that was started in November 1998.

ESD and use of Internet technology is guided by a comprehensive framework of legislation, TBS policies and guidelines, and within PWGSC by a policy infrastructure established through Deputy Minister Directives (DMDs) and other guiding instruments. PWGSC monitors the external policy infrastructure and has processes to establish websites and publish information on those sites. Although PWGSC has implemented these oversight measures, the audit found no controls to ensure that they are consistently applied when (a) sites are operated through private sector Internet service providers, and (b) information is updated or published on existing Inter/Intranet sites.

PWGSC currently lacks clearly defined and measurable indicators to support a comprehensive assessment of the department's evolution towards fully integrated ESD, or to support ongoing performance assessment of all discrete ESD initiatives. Development of such indicators may be complicated by the fact that PWGSC branches are evolving towards ESD and the use of Internet technology in different ways and at different rates.

Adherence to GOC requirements such as the Federal Identity Program, Internet Publishing Policies, the Official Languages Act, etc. are being monitored and overseen at the initial implementation phase by departmental areas charged with those responsibilities - Communication Branch and Internet/Intranet Services Group. Coordination and managerial oversight of specific initiatives is achieved through the requirement to report through the IM/IT governance committee structure, the establishment of specific strategic and working level committees and/or working groups involved with discrete ESD-related initiatives (e.g. the EP&S Steering Committee), and the management processes used within the recently reorganized GTIS organization and the other operating Branches of the department. As well, it is likely that the proposed Enterprise Project Office will have an oversight role over the GTIS projects it will coordinate.

The achievement of GOC and PWGSC ESD/Internet objectives will be highly dependent on the establishment of a supporting architectural infrastructure. GTIS is therefore under pressure to establish this infrastructure even though clear industry standards have yet to be established. Some business managers raised concerns that acceptance of new technology and standards would move too slowly to meet business needs and that standards would be mismatched to their business needs and available funding. Conversely, others were concerned that PWGSC would make decisions on direction and products too quickly such that supportability in the future would become an issue. As well, GTIS and PWGSC timeline and deliverables commitments made in regard to GOC objectives apply further pressure to embrace new architecture and infrastructure components. GTIS and PWGSC will be challenged in achieving and maintaining a workable balance between standardization and flexibility within its infrastructure.

The evolution towards ESD has already caused PWGSC to re-engineer many of its service delivery processes. GTIS has started and continues to restructure itself to better align its organization, people and products in support of ESD. Business Branches are beginning to evaluate ESD and the use of the Internet both in terms of opportunities and challenges to their organizations and business processes. As PWGSC proceeds, management must be cognizant of and establish controls to ensure continuity of services, client accessibility to Internet-enabled systems, and accuracy, timeliness and accessibility of information used within Internet-enabled systems. The department should ensure that sufficient resources and time are allocated to the re-engineering of these processes, that potential business opportunities are subjected to an appropriate evaluation, that accurate information is available as required, and that this re-engineering is characterized by effective horizontal communication and coordination within the department.

PWGSC has published specific directives on the risk management process for departmental information systems, including hardware, software, and facilities. PWGSC also has a Risk Management Framework (RMF) which is designed to ensure security risks associated with emerging systems, applications and hardware are identified and assessed. However, the RMF is not fully implemented and the risk management process is not being consistently applied for all new applications or major modifications sufficiently early to avoid a retro fit of security considerations. Finally, there is no monitoring/oversight of compliance to the process at this time. PWGSC should ensure the RMF is entrenched as an early step in the IM/IT governance process.

PWGSC has adopted a security configuration based on industry standards. Departmental assets are being protected by firewalls which have been configured based on PWGSC and GOC security policies and directives. However, security issues apply not only to information stored, processed or transmitted electronically, but also to the information systems, services and processes which might have an impact on this information. This extends security issues to Information Technology (IT) hardware and software, networks, telecommunications and other equipment that is interconnected, as well as to facilities in which this equipment is housed. Within PWGSC, the roles and responsibilities for the security aspects of each of these components are understood but audit results are inconclusive as to whether or not the lead role for security should reside within any component part or reside within a central group such as the Information Technology Security Directorate (ITSD). There is a risk that emphasis on one aspect (e.g. hardware) will promote a false sense that all security issues have been addressed.

PWGSC applies security mechanisms on a more reactive than proactive basis. As the availability of products and services on the Internet increases, so do opportunities for misuse and threats. There is a need for better awareness training in many areas surrounding the appropriate use of electronic networks and the risks involved with use of the Internet and ESD. Management needs to raise the department's overall security consciousness and continue to openly and visibly support a security-conscious operating environment at PWGSC.

While still on the security issues, PWGSC would enhance its network security position by confirming that there are no unauthorized ("rogue") modems on PWGSC workstations.

Conclusions

Delivery of government programs through electronic technologies is not a new concept, however ESD and the growing reliance on web-based technology is substantially different than what has been previously done. PWGSC is meeting this challenge in a number ways both within the business branches, which are looking at the use of Internet technology to achieve business objectives, and within GTIS which is attempting to establish its own business line as well as support PWGSC business requirements. PWGSC's success in realizing ESD will be contingent on the successful evolution and structured application of a comprehensive ESD-related management control framework.

As stated throughout this report, the MCF for using Internet technology in support of ESD and the achievement of business objectives is in transition. PWGSC has taken steps to improve its MCF for ESD in many key areas such as communications and coordination, IM/IT governance, compliance with applicable GOC and departmental requirements, management oversight, alignment of ESD with other priorities, development of architectural and infrastructure standards, re-engineering of relevant business processes, ESD security, and risk assessment. However, opportunities still exist to improve certain elements of PWGSC's MCF for ESD and use of Internet technology.

As PWGSC continues its evolution towards fully integrated ESD, the following key risks should be considered: the speed of change requires quick decision making processes; decisions on departmental and government wide standards will be made in an environment where there are no clear industry standards at this time; there will be pressure to implement new applications and drive ahead quickly applying pressure to the methodologies used to develop, test and implement IT applications; there will be increased pressure on PWGSC to demonstrate its ESD services are cost-competitive with similar services available from the private sector; and as was the case in the Year 2000 conversion project, it will be difficult to train and retain competent people - e-commerce is a fast-growing world wide phenomenon.

Recommendations

It is therefore recommended that:

1. *The ADM GTIS, via the IMC, complete in a timely manner the renewal of PWGSC's governance framework thereby stabilizing the department's IM/IT governance structures and processes.*

2. *The ADM, GTIS, via the IMC, ensure that the department's consolidated Risk Management Framework is entrenched as a required early step in the development and implementation of ESD-related Internet applications.*

3. *The ADM, GTIS, via the IMC, develop and implement an employee awareness program to address accountabilities, responsibilities and oversight in the areas of:*

   (A) the appropriate use of, and the risks involved when using, electronic networks.[1]

   (B) delivering services through external Internet service providers; and

   (C) ensuring continuous compliance with legislation and policies on established Inter/Intranet sites.

4. *The ADM, GTIS take steps to enhance its network security position by confirming that "rogue" modems within PWGSC are identified and eliminated.*

[1] Work on this recommendation has already started. The DM Directive on Network Use (DM 070) has already been published and follow-on awareness activities are underway.

1 Introduction

1.1 Authority for the Project

This audit was approved by the Audit and Review Committee as part of the 1999/2000 Audit and Review Branch (ARB) Plan.

1.2 Objectives

To assess the adequacy of the Management Control Framework (MCF) around the Department's use of Internet technology in support of Public Works and Government Services Canada (PWGSC) programs and Government of Canada (GOC) initiatives

1.3 Scope

The audit focused on the adequacy of the MCF related to the use of Internet technology to support Electronic Service Delivery (ESD) and other PWGSC business objectives (including support of GOC initiatives) in the key control areas of:

- *Definition and communication of objectives and goals*
- Project evaluation and approval
- Organizational structures
- Accountability, responsibility and roles definition
- Planning and risk assessment
- Policy, regulations, procedures and guidelines
- Safeguarding of assets and security
- Performance indicators and measurement
- Oversight

1.4 Approach

During the Preliminary Survey and Detailed Examination Phases, the audit team obtained and reviewed documentation and information from various sources including existing PWGSC paper-based files, and various PWGSC and external Inter/Intranet sites. This documentation included general information about the Internet and ESD, along with more specific information on PWGSC's efforts to evolve its MCF for using the Internet in support of the department's business objectives in an ESD environment. As well, the audit team obtained and reviewed available related central agency and PWGSC directives, policies, procedures and guidelines. In addition, the audit team conducted numerous interviews with PWGSC managers representing the major business lines within the department, as well as interviewing a representative of the Treasury Board Secretariat (TBS) with Internet/ESD related responsibilities. Finally, the audit team reviewed the following audit reports during the course of the audit:

- Review of Departmental IM/IT Planning and Governance Process
- Audit of the MCF for GTIS Services to External Clients
- Information Technology Security and Disaster Recovery Planning
- Review - Effectiveness of the Distributed Security Organization.

1.5 Background

"The Government of Canada has established a goal of making Canada the most connected nation in the world by the Year 2000. In support of this goal, governments are to show leadership by acting as model users of technologies, serving to demonstrate the advantages of electronic commerce (EC) and build trust.

Government use of electronic commerce to deliver services is growing: the Government of Canada has indicated that electronic commerce will become the preferred means to conduct business. Governments at all levels are turning to the Internet as a means of increasing the range, reach and availability of their services - available 24 hours a day, seven days a week, independent of location. As well, the costs of providing these services can be significantly reduced for both users and the government. Electronic delivery of government services will also facilitate the future integration of government services from different departments and different locations.

Electronic commerce can be defined narrowly or broadly. Broader definitions include any kind of transaction that is made using digital technology, including open networks (the Internet), closed networks such as electronic data interchange (EDI), and debit and credit cards. The narrower definition specifies that electronic commerce includes only transactions using Transmission Control Protocol/ Internet Protocol (TCP/IP). Electronic commerce is thus seen as an Internet application. While modest at this time, Internet based electronic commerce is projected to grow rapidly."[2]

The PWGSC Information Management Plan (IMP) 1998-2001 reflects the increased interest in electronic commerce and ESD to fulfill business objectives:

- The effectiveness of Automated Buyer Environment (ABE) in fulfilling its potential rests on the advancement of connectivity between ABE and client departments and suppliers. Priority projects within ABE include: electronic interfaces to MERX; electronic interfaces with clients for transmission of requisitions, attachments, requisition status and contract copies; electronic interfaces with translation services and interfaces to other procurement support tools.

- Government Operational Service (GOS) has identified within its major initiatives - an electronic commerce initiative to expand in the areas of electronic remittance, payment inquiries and payment issues.

[2]The Canadian Electronic Commerce Strategy, Industry Canada 1998

- As part of its common service mandate, Government Telecommunications and Informatics Services (GTIS) Branch plans to support common informatics services in the EC areas of: electronic directories, infrastructure components, electronic security and Government Electronic Data Interchange Service (GEDIS).

In April 1999, GTIS began a restructuring activity to address an initiative endorsed by the Treasury Board Strategic Advisory Committee (TBSAC) to create a centrally funded, procured and managed federated architecture supporting a secure GOC ESD channel.

An EC Steering Committee and a working group with GTIS, GOSB and SOSB representatives have been established. The group has commenced the Electronic Procurement and Settlement (EP&S) project with the objective of providing an integrated electronic end-to-end procurement through settlement process. As an initial step, an EC model using PWGSC as a model-user has been designed consisting of four components: electronic procurement, on-line purchasing, electronic settlement and enabling infrastructure. A presentation made to the Information Management Committee (IMC) on September 17, 1999 indicated that a high level Architecture Study was conducted for the EP&S project, and that a high level threat and risk assessment was completed in June 1999. A final recommendation was made to IMC to move forward with the formalized project. Once approved, the next steps in the process were to establish a project team, create a project charter, identify funding, and develop a procurement strategy, a detailed project plan and a governance process for the project.

2 Issues Examined

The complex nature of ESD and the fact that ESD is being undertaken from the starting point of existing infrastructures, processes and control frameworks is causing PWGSC to change the way it conducts business and the way it approaches service delivery. The end-to-end nature of the EP&S project is evidence that functions that were once separate from each-other are now coming together in the ESD environment. As a result, the evolving MCF around ESD and use of the Internet is both broad and multifaceted. With this in mind, and while maintaining its focus on the evolving MCF, the audit team explored the broad range of management control issues identified below. Each of these issues was identified and examined using an industry accepted audit methodology applicable to an organization's IM/IT function.

- Definition and Communication of Objectives and Goals
- Coordination and Communication
- IM/IT Governance
- Policy/Legislative Framework and Conformity
- Aligning ESD with other PWGSC Priorities
- Oversight
- Architecture/Infrastructure Standards
- Business Process Re-engineering
- Risk Assessment
- Security

3 Findings, Conclusions and Recommendations

This section presents audit findings which are organized by the audit issues outlined in the prior section, along with audit conclusions and recommendations.

3.1 Definition and Communication of Objectives and Goals

PWGSC should ensure its objectives for ESD and the use of Internet technology are well defined, clearly communicated, and consistent with similar objectives at a GOC level. Similarly, the ESD-related objectives of the various PWGSC Branches should be consistent with and supportive of the broader departmental ESD-related objectives.

Audit results indicate that PWGSC's objectives for ESD using Internet technology are well defined and communicated both at the government-wide and departmental levels. Overall, there is a recognizable consistency between the objectives identified at the government-wide level and the stated PWGSC objectives for the use of Internet technology and ESD. Similarly, the goals of the various PWGSC Branches articulated in business and strategic plans are consistent with and support the broader PWGSC objectives.

3.2 Coordination and Communication

PWGSC should have mechanisms in place to ensure departmental ESD-related interactions with external stakeholders, as well as internal ESD-related interactions within the department, are effectively coordinated and characterized by open and reliable communications.

3.2.1 Coordination and Communication with External Stakeholders

PWGSC has implemented mechanisms to manage and coordinate ESD-related activities and initiatives with external stakeholders, including TBS, other government departments (OGDs), and the private sector.

PWGSC and TBS are jointly involved in the design, development and implementation of the Federated Architecture (also known as the Federated Infrastructure), a multi-layered ESD-enabling Internet-based infrastructure. The Assistant Deputy Minister (ADM), GTIS is a member of IM/IT Management Board (IMB) which is the strategic oversight committee for the Federated Architecture. PWGSC is also represented on working groups addressing specific aspects of the Federated Architecture initiative (e.g. Public Key Infrastructure (PKI)). Both TBS and the ADM, GTIS are communicating and promoting the Federated Architecture to the private and public sectors through events such as the Electronic Commerce symposiums held recently in the National Capital Area. GTIS also recently created the Strategic Services Sector (SSS). The SSS includes three Directorates (Portfolio Strategies) to support government departments in their program delivery, and three Directorates (Technology Partnerships) to explore partnership opportunities with the private sector in the delivery of the Federated Architecture. Although the SSS is a new organization and therefore has no history within PWGSC's

MCF, given that it is a forward-looking organization interested in the longer-term strategic aspects of ESD and the role PWGSC will play in supporting ESD across the federal government, the SSS is a positive addition to the department's MCF for ESD.

On the whole, coordination and communication between PWGSC and TBS, OGDs and the private sector are evolving positively as work on initiatives such as the Federated Architecture continues.

3.2.2 Internal Coordination within PWGSC

Within PWGSC, the work undertaken in support of the Federated Architecture will be combined with business branch infrastructures and corporate applications to achieve PWGSC ESD business objectives. GTIS has begun to implement measures to improve coordination and communication within the GTIS sectors, and with and among business branches. However, opportunities still exist to improve the overall MCF relating to internal coordination, especially considering that much of the MCF is in the process of being implemented.

PWGSC business branches are now considering Internet technology and ESD alternatives to achieve their business objectives. Proposals and initiatives are being overseen by specific project managers who report to branch management committees. Portfolio Executives within Application Management Services (AMS) interface with project managers and often attend business planning and management meetings. Continuity of communication and coordination flows from and to business branches through the GTIS sector activities and meetings.

GTIS specialists are often involved in application development projects either as the team producing the required system (analyses, programming, quality control, etc) or as advisors and project coordinators when the development work is externally contracted. In the past, audits have found that GTIS involvement in projects is inconsistent and in some cases not timely.

The IM/IT governance framework, through its committee structure, also provides a forum for horizontal and corporate planning, coordination and communication. This IM/IT governance framework, which includes both a governance structure and governance process, is currently being reviewed.

An Architecture and Engineering Steering Committee (AESC) has been established which will evaluate new project proposals for technical feasibility and appropriateness within the PWGSC architecture. Centres of expertise (COEs) consisting of identified specialists in specific functional areas will support the AESC by reviewing proposals submitted by business branches, other GTIS sectors and those involved with the Federated Architecture project. Early indications are that COE's will establish standards for the documentation of requirements.

Also, a recent proposal calls for the establishment of an Enterprise Project Office (EPO) which would facilitate the overall coordination of GTIS IM/IT projects. The EPO would be responsible to provide among other things a bridging mechanism between Sectors and enterprise-wide strategic and operational plans, facilitate cross-sector initiatives, and establish and maintain an inventory of GTIS projects. While conceptually sound as a coordinating mechanism, audit results indicate the extent of coordination to be performed by the EPO is still to be finalized.

GTIS is hosting one-day retreats with other PWGSC business branches to improve its communications with internal clients and to better understand their IM/IT requirements. Although not yet completed, these retreats are a positive addition to the communications element of the overall departmental IM/IT MCF.

PWGSC has also established an infrastructure and processes to coordinate the creation of Inter/Intranet sites and to ensure information published on those sites adheres to federal government and departmental requirements. Communication Branch monitors external web publishing policies and directives and has produced and maintains a web publishing guide. The Internet/Intranet Services group within GTIS provides webpage assistance and ensures that the publishing guide and other departmental policies and Internet procedures are addressed prior to establishing an Inter or Intra net site. Internet/Intranet Services has also produced an inventory of web sites and applications.

Many of these framework elements are either new, under review or still to be implemented. As such, ongoing GTIS executive support and continued work by all involved will be required to ensure that the objectives of these communication and coordination activities are achieved.

3.3 IM/IT Governance

PWGSC should have effective management processes and decision-making mechanisms in place to govern the evolution and implementation of IM/IT and ESD within the department and, to the extent that PWGSC is a common service agency on behalf of the GOC, at the higher government-wide level. These processes and mechanisms should be sensitive to and adaptable to pressures stemming from the rapid pace of IM/IT evolution.

IM/IT within PWGSC is managed through a departmental governance framework which is often supplemented by similar frameworks at the branch level. While the specifics of these branch-level governance frameworks may differ, generally there is a branch IM/IT committee which either reports to or is overseen by the branch ADM. These committees, which usually act as a recommending or decision making body for the ADM, are often supported by lower level committees established to oversee specific initiatives or projects. Individuals manage operational IM/IT activities or act as project managers for approved new initiatives. Corporate or horizontal projects may be referred to the corporate IM/IT governance structure for information, funding or approval.

PWGSC's corporate IM/IT governance framework is in transition. The current framework includes the senior level IMC as the key decision-making body with respect to the department's IM/IT direction. IMC was supported by the Business, Information and Technology Alignment Sub-Committee (BITASC) and the Infrastructure Sub-Committee (ISC). However, BITASC is currently on hold pending further direction from IMC. The recently established AESC will oversee, coordinate and manage the evolution of PWGSC's IM/IT architecture, infrastructure and security at the enterprise level to ensure support of PWGSC business and government-wide requirements in an adaptive manner. The AESC replaces the previous ISC and various sub-committees and working groups which reported to the more senior committees.

Corporate projects or initiatives such as the EP&S Project, and GTIS Government of Canada projects such as the Secure Channel Project, are managed by project managers who report to steering committees. The steering committees either report directly to IMC or through the GTIS management structure to IMC.

The corporate governance structure, the relationship of branch processes to the corporate structure, and roles and responsibilities of entities in the governance process were under review and being redefined in late 1998. This review occurred prior to the recent reorganization of GTIS and the establishment of the new AESC. Consequently, the proposal to renew the governance framework which resulted from the review is out of date. Therefore, there is no up-to-date plan to guide the renewal of the overall PWGSC IM/IT governance framework and outline the roles and responsibilities of the various entities involved. This introduces a risk that the effectiveness of IM/IT governance within PWGSC may be adversely affected until a renewed governance framework is agreed to and implemented. The renewal of the IM/IT governance framework may also provide an opportunity to strengthen the degree to which branch IM/IT governance processes are integrated with the departmental IM/IT governance process.

As indicated earlier, Portfolio Executive positions exist within GTIS AMS to provide other operating branches a point of contact for obtaining GTIS services. These positions may provide liaison between GTIS and individual branch IM/IT governance processes. However, in an attempt to improve customer access to GTIS services, GTIS has recently adopted a "no wrong door" position indicating that GTIS services may be accessed via various entry points. Audit results are inconclusive as to the impact this "no wrong door" position will have on the overall departmental IM/IT governance process or on the communication and coordination function performed by Portfolio Executives.

In contemplating a renewed IM/IT governance framework, management may wish to consider two specific concerns encountered during this audit. First, that the rapid pace of technological change and the nature of electronic service delivery may require a re-evaluation and a streamlining of relevant management and operational decision-making processes in order to realize a more integrated holistic IM/IT decision-making process. Second, given that ESD may reduce or eliminate boundaries which have traditionally existed between organizations (or branches) prior to the Internet and ESD, new funding models may be required in order to ensure the costs and benefits of ESD-related IM/IT decisions are appropriately managed.

3.4 Policy/Legislative Framework and Conformity

PWGSC should have a comprehensive departmental infrastructure of policies and other guiding instruments which is consistent with and supportive of the existing regulatory framework of current legislation and TBS policies. PWGSC's departmental policy infrastructure should itself be supported by mechanisms to ensure compliance with mandatory external and departmental requirements.

From a government-wide perspective, ESD and the use of Internet technology is currently guided by a comprehensive framework of GOC legislation and TBS policies and guidelines. Through Deputy Minister Directives (DMDs) and other guiding instruments, PWGSC has established a departmental policy infrastructure which is consistent with and supportive of the framework of legislation and TBS policies and guidelines (e.g PWGSC supports compliance to the Official Languages Act through its Policy on Using Official Languages on Electronic Networks). Through this departmental policy infrastructure, PWGSC has assigned accountabilities and responsibilities for various aspects of the evolving MCF for ESD and the use of Internet technology within the department.

PWGSC's Communications Branch currently monitors the external component of this policy infrastructure on behalf of the department, and is available to provide information and assistance to the business branches in implementing appropriate policies.

The GTIS Internet/Intranet Services group works with individual publishers and Branch/Regional Web Administrators throughout the creation and maintenance of their information holdings. As partners with Corporate Communications, they provide technical advice, software and support. Corporate Communications advises Internet/Intranet Services as to the effective use of this medium, policy considerations, and standards for federal government Web sites. Internet/Intranet Services webmaster responsibilities include: overall site management, moving files into production, design assistance, software (supported products) for publishers, publishing software support, web site statistics (monthly), scripting for forms and other uses, tailoring search facilities, training, and suggestions and possible sources for training. These activities provide a level of assurance that information published on those sites adheres to federal government and departmental requirements. Assuming these processes are followed, there are sufficient controls to ensure site creation is managed in a coordinated manner and to ensure published information is compliant with existing requirements. However, risks exist in how this policy infrastructure is operationalized within the department.

Business managers seeking cost-effective IM/IT solutions to business needs can currently have Inter/Intranet sites created using private sector Internet service providers (ISPs), rationalized on the basis that costs for sites established in this manner both satisfy their business requirements and yield savings (relative to the cost of obtaining the same services within PWGSC). Accountability for the management of websites and web applications, whether internally operated or provided through an ISP, is the responsibility of the designated business manager. However, the internally operated websites and applications have a greater degree of oversight by various corporate organizations, such as Communication Branch and Internet Services Group,

and are less likely to operate in an undetected non-compliant mode brought about by the dynamic environment with changing standards. Audit results indicate there is less oversight of subsequent changes and enhancements made to already-published information on websites operated in both the private sector or within the PWGSC infrastructure.

In addition, employee access to electronic networks is governed by the PWGSC policy infrastructure. Departmental employees given access to electronic networks (which includes the Internet), are responsible for using the Internet in a responsible manner by observing applicable departmental and GOC legislation, policies and directives. Managers of these employees are responsible for ensuring their employees are aware of relevant communications policies, guidelines, directives and legislation. Given the risks of inappropriate use of the Internet by employees (whether intentional or not) and the associated managerial responsibilities for ensuring employee awareness, management may wish to reinforce the appropriate use of Internet technologies by designing and implementing a vigorous departmental awareness program.

3.5 Aligning ESD with other PWGSC Priorities

PWGSC should have mechanisms in place to ensure that the evolution of ESD and the implementation of Internet-based service delivery options are successfully aligned with other stated departmental priorities.

As PWGSC evolves towards a more fully integrated ESD environment, management must ensure this evolution is planned, executed and evaluated in a continuous and well-managed fashion. However, current PWGSC strategic and business plans lack clearly defined, measurable, indicators to support the assessment of this evolution, or to support ongoing performance assessment of all discrete ESD initiatives. Such metrics are necessary if PWGSC is to be able to evaluate the success of its overall evolution towards a more fully integrated ESD environment, as well as "the success of a specific initiative in meeting core public policy objectives and efficient, effective delivery objectives for individual clients."[3]

The EP&S Project is an initiative which crosses business branch boundaries and has a multi-branch steering committee. However, for other initiatives PWGSC branches are evolving towards ESD and the use of Internet technology in different ways and at different rates. This emphasizes the need for effective coordination and communication mechanisms in support of the learning organization objective, and an integrated service delivery model providing "specific service packages tailored to client needs."[4] As already identified, there are many coordination and communication mechanism in place or being implemented within GTIS and the business branches. Successful operation of these mechanisms will not only support effective and efficient development, implementation and operation of ESD and Internet applications, but they will also support the achievement of other departmental objectives, as well as the "no wrong door" client service objective of GTIS.

[3]PWGSC Business Plan 1998/99 to 2000/01

[4]PWGSC 1999-2000 Estimates, Part III - Report on Plans and Priorities

3.6 Oversight

PWGSC should have effective departmental oversight and feedback mechanisms in place to monitor and report on the evolution of ESD, and the development and implementation of all ESD/Internet related IM/IT solutions. PWGSC currently uses various mechanisms to oversee its ESD and internet-related initiatives and activities. However, there is still room to improve the oversight function.

Oversight is provided through the hierarchy of committees within the department's governance structure and processes, by specific committees or working groups involved with discrete ESD-related initiatives, and by the management processes used within the recently reorganized GTIS organization and the other operating Branches of the department.

Within the existing PWGSC IM/IT governance structure, IMC and BITASC (until it was put on hold) provided the highest level of oversight of strategic and operational ESD and internet-related initiatives and activities for the department. A review of available IMC minutes indicate the committee has been involved in overseeing relevant IM/IT initiatives such as PWGSC's policy on the use of electronic networks (DMD 70) and the EP&S (or E-Commerce) project. IMC has also during the recent past been focused on its standing agenda items, namely Year 2000 Contingency Planning and status of Year 2000 readiness, and the Office Infrastructure Renewal (OIR) Project.

Subject to implementing the proposed re-engineered governance framework, it is expected that oversight of an administrative nature will be provided by the proposed Enterprise Project Office for all projects in GTIS.

Oversight of the EP&S project is also provided by the AESC under the general direction of the DG, Secure E-Commerce and Emerging Technologies, GTIS. In addition, an EP&S Strategic Advisory Committee, with representation from across the department, supports the AESC.

Communications Branch, the Internet/Intranet Services Group, along with those who have been assigned web-publishing responsibilities via PWGSC's Web Publishing Guide, provide oversight over the creation of Internet sites and compliance with information publishing requirements at those sites. However, as noted earlier, certain control improvement opportunities exist with respect to the management of Internet site creation and the subsequent publishing of information on PWGSC sites.

Employee use of the Internet is also monitored by the Information Technology Security Directorate (ITSD) within GTIS. This is discussed further in the subsequent sections of this report on Risk Assessment and Security. As well, managers are responsible under DMD 70 to monitor, as part of day-to-day supervisory activities, the use of information and technology to ensure these resources are used productively, effectively and acceptably for business purposes.

Although PWGSC has implemented these oversight measures, the use of private sector ISPs for Internet sites involves a risk that existing oversight measures will not adequately address sites

created by means other than the current IM/IT governance processes. Similarly, the publishing or updating of information on existing Internet sites, when performed outside the existing process for web-publishing, involves the risk that this information may not be subjected to an adequate oversight function.

3.7 Architecture/Infrastructure Standards

As ESD/Internet applications are highly dependent on the architectural infrastructure upon which they are built, PWGSC should have effective processes in place to establish and apply ESD/Internet-related architecture and infrastructure standards to emerging systems and application development projects.

GTIS, as part of its restructuring process, has created specific organizational units to monitor industry trends and new directions. As stated previously, the AESC evaluates the technical feasibility and appropriateness of new projects and initiatives arising from clients within and outside of PWGSC. GTIS has established project teams to address the Federated Architecture and the associated architecture and infrastructure requirements and standards.

Being at the leading edge of technology has associated risks. Business managers interviewed were concerned that acceptance of new technology and standards would move too slowly to meet business needs within the department and that standards would be mismatched to their needs and available funding. Certain technical managers were concerned that they were under pressure to make decisions on direction and products too quickly and that supportability in the future might become an issue. Similar observations have been noted during past audits. However, as many enablers of e-commerce are new, clear standards have yet to be determined in many areas.

Further pressure is also being applied to embrace new architecture and infrastructure components by the timeline and deliverables commitments GTIS and PWGSC have made in regard to GOC objectives.

3.8 Business Process Re-engineering

The objective of delivering government programs using technology including the Internet has already had an impact on PWGSC and how it does its business.

GTIS has taken a proactive approach to GOC ESD objectives. It has actively pursued a role in the definition and implementation of a Federated Architecture model. It has accepted responsibility and is being funded to deliver various components of the model. The restructuring of GTIS, is a realignment of its business units to reflect the emphasis on ESD objectives. GTIS is also addressing its GOC commitments by initiating special projects such as the Secure Remote Access (SRA) Project, the PKI Project and the Secure Channel (SC) Project. Projects facilitate bringing the required resources together, assigning responsibilities and accountabilities to individuals, and focusing efforts to achieving objectives within specified timeframes. Projects also make it easier to establish partnerships with the private sector, considered necessary to achieving departmental and GOC objectives.

However, there are areas of risk for GTIS and therefore to PWGSC.

While servicing GOC initiatives, GTIS must still recognize and deal with internal ESD requirements. Business branches will be expecting GTIS to provide the architecture/infrastructure, organization and resources to support their initiatives. GTIS will have to strike a balance between internal and external requirements. Funding of PWGSC activities may be an issue. While some of the costs of establishing ESD will be funded through GOC initiatives, there will still be other costs which are new, both ongoing and start-up, that must be absorbed within the department or by the particular business branches. Existing problems with costing and allocating project costs will have an effect on how ESD is implemented in PWGSC.

Successful restructuring of the organization and increased operation within a matrix management environment will require consistent visible commitment by management, and buy-in by GTIS employees. GTIS has established an Intranet site to communicate information to all PWGSC employees. It has established project teams and work groups to drive the restructuring process. The ADM, GTIS has been visible in delivering and communicating the new focus and direction. Given the extent to which the GTIS organization and culture is changing, it is imperative that these types of activities continue.

As PWGSC re-engineers its processes to adapt to emerging ESD and Internet-related IM/IT solutions, it must be cognizant of and establish controls to ensure continuity of services, client accessibility to Internet-enabled systems, and accuracy, timeliness and accessibility of information used within Internet-enabled systems. The department should ensure that sufficient resources and time are allocated to the re-engineering of these processes, that potential business opportunities are subjected to an appropriate evaluation, that accurate information is available as required, and that this re-engineering is characterized by effective horizontal communication and coordination within the department.

3.9 Risk Assessment

PWGSC should have effective risk management mechanisms in place to manage the various types of risks which stem from ESD and the use of Internet technology including (1) business-related risks (e.g. risks stemming from the implementation of ESD solutions that could jeopordize the achievement of business/program objectives), (2) IM/IT governance risks (e.g. risks that could undermine PWGSC's corporate IM/IT governance process), and (3) IM/IT security-related risks (e.g. security-related risks which accompany discrete IM/IT ESD projects).

Our review was performed in each business branch and in GTIS to identify risk assessment and management practices in relation to IM/IT and specifically ESD applications, projects and initiatives. The review revealed that PWGSC has a Risk Management Framework (RMF) which is designed to ensure security risks associated with emerging systems, applications and hardware are identified and assessed. Developed by ITSD, the RMF consists of standards, procedures, guidelines and deliverables for assessing and managing security risks. Use of this RMF should

provide assurance that confidentiality, integrity, availability and accountability requirements of new and modified information systems and components are met.

Key components of the RMF include the preparation of a Statement of Sensitivity and a Threat and Risk Assessment, key requirements under the departmental Security Policy. There is also a Quality Assurance function where ITSD or an ITSD-contracted resource performs an accreditation and certification of the system, hardware component or service.

The RMF may be used as part of the technical feasibility and appropriateness assessment activities identified in the Architecture and Engineering governance process. ITSD is one of the COEs and therefore one area of consideration for the AESC. Applying the RMF may also, if done early in the system development life cycle, assist analysts, developers, testers and operational staff in implementing appropriate security precautions. Ultimately it should assist the business manager of the system, product or service to address security accountabilities.

Currently the RMF is not fully implemented - it has yet to be published. Also, the risk management process is not being consistently applied for all new applications or major modifications. ITSD is not always involved sufficiently early to avoid a retro fit of security considerations. Finally, as there is no monitoring/oversight of compliance to the process at this time, managers are to be held accountable for security.

Assessing IT risk is one element of a broader set of risk management activities. Other elements include establishing a central management focal point, implementing appropriate polices and related controls, promoting awareness, and monitoring and evaluating policy and control effectiveness.

The management of Year 2000 conversion activities in PWGSC included a standardized, cyclical, and holistic assessment, management and reporting of risks. All risks associated with the project were identified and evaluated including environmental, external, business, legal and infrastructure risks. There was a rigorous risk assessment around the Year 2000 process with an assessment and management structure. On a continuous basis, Year 2000 critical systems were examined, reported on, monitored and controlled.

While there is some form of risk management in each business branch, planning and governance evidence gathered, within the resource and time limitation of this audit, did not identify a process approaching the rigor of that used by the Year 2000 program office.

TBS policy specifies a requirement to identify and reduce or eliminate risks to its property, interests and employees, to minimize and contain the costs and consequences in the event of harmful or damaging incidents arising from those risks, and to provide for adequate and timely compensation, restoration and recovery.

Within PWGSC, the ITSD is the focal point for IM/IT risk management activities. As part of the Security Policy, PWGSC has published specific directives related to the risk management process for departmental information systems, including hardware, software, and facilities.

Industry standards suggest a higher degree of risk is associated with systems used for ESD. Use of an Internet solution for a business requirement introduces greater threats of computer intrusion, fraud, and disruption.

3.10 Security

ESD and use of Internet technology, by its widespread access and open characteristics, increases risks to confidentiality and integrity of information, and accessibility to information and systems. The growing use of Internet technology increases the need for a government-wide secure electronic infrastructure. For Canadians to use this new technology they must trust that these potential risks are managed and their information is being appropriately safeguarded.

According to the TBS Information Technology Security Standard Policy (1995-08-29), "Information technology security is intended to ensure the confidentiality of information stored, processed or transmitted electronically; the integrity of the information and related processes; and the availability of information, systems and services. This comprises the security of information technology hardware and software, networks, telecommunications and other equipment that is interconnected, and facilities in which the equipment is housed."

Security issues surrounding ESD solutions may emerge from areas identified above and for the processes which support these components. The assurance of a highly secure ESD environment will require that each of these areas is reviewed as part of the risk management process.

Interviews indicate that within PWGSC roles and responsibilities for the security aspect for each of the various components are understood. However, there remains a question as to whether or not the lead role for security should reside within any component part or reside within a central group such as ITSD. There is a risk that emphasis on one aspect, such as hardware, will promote a false sense that all security issues have been addressed.

GTIS has been involved in many aspects of implementing security related "enablers" on behalf of the GOC with such projects as the SRA project and SC Project.

PWGSC has implemented industry standards to protect the network via firewall architectures and systematic monitoring and reporting on traffic through these firewalls. Public access websites are isolated from the departmental network and secured by a dedicated firewall. An Intrusion Detection pilot project is also currently underway.

Although progress is being made, application of security mechanisms continues to be more reactive than proactive. Potential risks continue to exist in the following areas:

- transfer of sensitive or classified information by electronic mail;
- deterioration in network performance caused by personal use of corporate resources;
- policy on PKI use by employees needs to be developed;
- unidentified and unauthorized "rogue" modems allow unsecured access;

- firewall disaster recovery plans have not been tested;
- oversight of websites operated outside of the PWGSC infrastructure;
- adequacy and numbers of expert resources, especially in the area of PKI;

As the availability of products and services on the Internet increases, so do the opportunities for misuse (whether intentional or not) by employees. Several managers expressed concern about transfer of sensitive or classified information by electronic mail and the potential for embarrassment when items are sent in plain text through the firewall to the Internet. While there is a Certificate Policy and there are Certificate Practices Statements, concern was expressed by some interviewees, that managers would share their private keys with support staff (as has been done in the past with passwords). The possible deterioration of network performance through large file downloads and transfers was cited. These observations indicate a need for better awareness training in many areas surrounding the risks involved with the use of the Internet and ESD.

A more systematic approach to security awareness should be considered. Management needs to raise the department's overall security consciousness and continue to openly and visibly support a security-conscious operating environment at PWGSC. Consideration should be given to system sign-on greetings that educate and support security issues. This will become more important as the widespread use of PKI and non-repudiation become a reality within the PWGSC environment.

Although hardware and software have been procured to conduct a sweep of modems in use in the department, there has been no commitment of resources to carry out the activity. The presence of "rogue" modems leaves the departmental network vulnerable to penetration by unidentified and untraceable sources who are able to circumvent the firewall through this means. Management should allocate resources to this task on a priority basis.

While a firewall disaster recovery plan does exist, this plan should be revisited and tested on a regular basis. This will provide assurance that loss of service will be minimized and that all of the elements of the plan reflect the current operating environment. At a minimum, the plan should be tested as part of the Year 2000 strategy.

Internet solutions have been sought outside the GTIS network, and are currently running applications with outside suppliers. Although exceptions are to be approved at the IM/IT committee level, standards need to be developed and applied as to what minimum security requirements are necessary for such applications to be certified.

ESD growth will also be accompanied by a high demand for personnel with experience managing, maintaining and supporting the various components in the security framework. This is presently being experienced by GTIS in the area of PKI, where there is considerable turnover. It is important that this element be factored into the risk assessment process when deploying these new services and promoting current products. GTIS acknowledges this problem and has stated that, particularly in the area of PKI, "personnel strategies need to be reviewed." GTIS has also

indicated that the pool of available CS' will be impacted by the requirement for "secret" security clearance to work on Secure ESD applications.

3.11 Conclusions

Delivery of government programs through electronic technologies is not a new concept, however ESD and the growing reliance on web-based technology is substantially different than what has been previously done. PWGSC is meeting this challenge in a number ways both within the business branches, who are looking at the use of Internet technology to achieve business objectives, and within GTIS which is attempting to establish its own business line as well as support PWGSC business requirements.

As stated throughout this report, the MCF for using Internet technology in support of ESD and the achievement of business objectives is in transition. Many MCF elements were new or being reviewed during the audit. In this context, the audit team has established the following audit conclusions:

Objectives related to ESD and the various enabling sub-components have been identified and communicated. Roles and responsibilities have been and are being assigned, but role definition continues as the department's governance framework evolves.

PWGSC has recently implemented new measures to improve the coordination and communications surrounding ESD-related initiatives within PWGSC. These measures will affect both PWGSC's relationships with external stakeholders (TBS, OGDs and the private sector) as well as relationships within the department itself. However, PWGSC can improve coordination by establishing the Enterprise Project Office and ensuring that it acts as a central point for tracking, monitoring and reporting to senior management on emerging ESD initiatives and projects.

Through DMD's, PWGSC has established an accountability framework for ESD-related matters. However, use of private sector Internet service providers may not be adequately addressed by this framework. If business managers continue to use external ESD delivery mechanisms, PWGSC should ensure its accountability framework addresses issues such as cost-competitiveness, security, and compliance to requirements. Currently, consolidated oversight in these areas appears to be lacking.

The planning and governance processes previously used to control IM/IT initiatives continues to be reviewed and revised. There appears to be a reliance on GTIS to ensure horizontal/corporate activities and issues are brought forward to the IMC. PWGSC should complete the renewal of its IM/IT governance framework thereby stabilizing its IM/IT governance structures and processes.

While PWGSC needs to have clearly stated architectural and infrastructure standards for emerging IM/IT initiatives and projects, these standards must also be flexible enough to allow for the development of IM/IT solutions which meet the needs of business

managers. PWGSC must achieve a workable balance between standardization and flexibility.

Adherence to GOC requirements such as the Federal Identity Program, Internet Publishing Policies, the Official Languages Act, etc. are being monitored and overseen at the initial implementation phase by departmental areas charged with those responsibilities - Communication Branch and Internet/Intranet Services Group. The MCF over existing sites was found to be less vigorous, particularly in the area of oversight. This poses certain risks for the department.

Products necessary to support ESD applications and GOC objectives are at varying stages of completion. Projects such as the GTIS PKI Project and the SRA project have recently been launched, accredited and made fully operational. Whereas, the SC project is just getting started.

All emerging ESD applications and initiatives should be subjected to a thorough risk assessment, including all instances when use of an external ISP is proposed. However, PWGSC's CRMF does not appear to have been fully adopted as an integral step in the overall IM/IT governance process. PWGSC should ensure the RMF is entrenched as an early step in the IM/IT governance process.

PWGSC has adopted a security configuration based on industry standards. Departmental assets are being protected by firewalls which have been configured based on PWGSC and GOC security policies and directives. However, security issues apply not only to information stored, processed or transmitted electronically, but also to the information systems, services and processes which might have an impact on this information. This extends security issues to IT hardware and software, networks, telecommunications and other equipment that is interconnected, as well as to facilities in which this equipment is housed. Within PWGSC, the roles and responsibilities for the security aspects of each of these components are understood, but audit results are inconclusive as to whether or not the lead role for security should reside within any component part or reside within a central group such as ITSD. There is a risk that emphasis on one aspect (e.g. hardware) will promote a false sense that all security issues have been addressed.

While still on the security issues, PWGSC would enhance its network security position by confirming that there are no "rogue" modems on PWGSC workstations and by establishing an employee awareness campaign about the risks involved in, and the appropriate use of, electronic networks (including the Internet).

As PWGSC continues its evolution towards fully integrated ESD, the following key risks should be considered: the speed of change requires quick decision making processes; decisions on departmental and government wide standards will be made in an environment where there are no clear industry standards at this time; there will be pressure to implement new applications and drive ahead quickly applying pressure to the methodologies used to develop, test and implement IT applications; there will be increased pressure on PWGSC to demonstrate its ESD services are

cost-competitive with similar services available from the private sector; and as was the case in the Year 2000 conversion project, it will be difficult to train and retain competent people - e-commerce is a fast-growing world wide phenomenon.

3.12 Recommendations

It is therefore recommended that:

1. *The ADM GTIS, via the IMC, complete in a timely manner the renewal of PWGSCs governance framework thereby stabilizing the department's IM/IT governance structures and processes.*

2. *The ADM, GTIS, via the IMC, ensure that the department's consolidated Risk Management Framework is entrenched as a required early step in the development and implementation of ESD-related Internet applications.*

3. *The ADM, GTIS, via the IMC, develop and implement an employee awareness program to address accountabilities, responsibilities and oversight in the areas of:*

   (A) the appropriate use of, and the risks involved when using, electronic networks.[6]

   (B) delivering services through external Internet service providers; and

   (C) ensuring continuous compliance with legislation and policies on established Inter/Intranet sites.

4. *The ADM, GTIS take steps to enhance its network security position by confirming that "rogue" modems within PWGSC are identified and eliminated.*

[6] Work on this recommendation has already started. The DM Directive on Network Use (DM 070) has already been published and follow-on awareness activities are underway.