CEAA Strategic IT Plan 2010 - 2015

Par
Alexandre Tardif

Rapport de travail dirigé présenté à l'ENAP,
en vue de l'obtention de la Maîtrise en administration publique
option pour analystes

Agence Canadienne d'évaluation environnementale

Ottawa

Avril, 2010

Version Control			
DESCRIPTION/CHANGES	**VERSION**	**DATE**	**NAME**
First Draft	1.0	2009-10-15	Alex T.
Updates	1.0	2009-11-16	Alex T.
Updates	1.0	2009-12-14	Alex T.
Updates	1.0	2010-01-11	Alex T.
Updates	1.0	2010-01-25	Alex T.
Updates	1.0	2010-02-08	Alex T.
Updates	1.0	2010-02-22	Alex T.
Updates	1.0	2010-03-01	Alex T.

The IT Plan will be subject to an annual update. The process and timing will be aligned with the business planning cycle.

Table of Contents

List of Figures

List of Tables

Appendix

Executive summary

Change is the only constant we can predict with certainty, and as the rate and pace of change accelerates, Government and the Canadian Environmental Assessment Agency (CEAA) are challenged to respond with more efficiency to the growing needs and services to Canadians. The preeminence of the environment on the citizen & government agenda and the need for CEAA to deliver results and meet department's strategic outcomes will place even greater demand on CEAA's Information Services Group.

In alignment with these demands, the Information Services Group is committed to deliver an IT (Information Technology) Plan to enable the achievement of the Agency's programs and departmental strategic goals. The challenge of delivering Enterprise wide IT solution department wide services will require a higher level of process and service integration across CEAA.

In order for CEAA to align with and meet departmental priorities and comply with Government-wide IM (Information Management) & IT policy strategies, the CEAA IT Plan follows the published model by Treasury Board of Canada (TBS).

In their direct accountability to the Deputy Minister, its clients and colleagues, the mandate of CEAA Information Services Group is to support the achievement of departmental priorities and strategic goals by providing integrated service delivery, support and direction in the areas of IM and IT to its clients and colleagues.

The CEAA Information Services Group must also strive to reach harmony between being effective, being efficient and compliant based upon availability of CEAA Information Services Group resources (people, processes, regional & national requirements, budget and technology).

In addition, in order to meet his objectives, CEAA Information Services Group will review & manage on a regular basis his annual Service Level Agreement with Environment Canada for IT shared services.

The scope of this document focused on IT only. Although CEAA Information Services Group also manages IM related activities, as IT activities and tools enable IM at the Agency. A separate 5 year IM strategic plan has been completed in 2009 (internal reference RDIMS document number: 55603)

The update cycle of this IT plan is scheduled to be synchronized with the Agency Corporate planning review in September and fiscal year end.

Preface (Situational Analysis)

The Management Accountability Framework (MAF) round VI (2008-2009) is an evidence-based exercise that evaluates three lines of evidence under information technology: leadership, planning and value. Each of these three areas has a two-dimensional perspective that includes: horizontality across government and downward into the organization.

Since MAF IV (2006-2007) a significant collaborative effort was undertaken to raise awareness and take steps to improve the planning culture across government. These efforts included presentations at both the 2007 and 2008 CIO Executive Summit, the 2007 TBS CIO Branch MAF measures blog pilot, the 2008 TBS CIO Branch Wiki collaboration on MAF measures, TBS CIO Branch Information Technology management governance workshops, collaboration between TBS and PWGSC on developing a common and shared services adoption plan, bilateral discussions with organizations and six MAF VI training sessions.

The resulting Information Technology Plan guide that accompanied the MAF VI submission package is the key assessment tool for evaluating the content of Information Technology plans. The Information Technology Plan guide is more rigorous than the criteria used to evaluate Information Technology plans in MAF V. Also, MAF VI evaluates the maturity of the planning culture in the organization with emphasis on the governance practices and processes that guide Information Technology investment decisions. Therefore, it is possible that what was an acceptable or strong rating in planning in MAF V might not be evaluated at the same rating in MAF VI and resulting overall ratings could be lower.

Delivering value to the organization through the use of common and shared services continues to be a significant factor in the assessment for MAF VI. Also MAF VI evaluates the maturity of management practices in the areas of Information Technology service costing, asset management, performance measurement and performance reporting. Therefore, it is possible that an acceptable or strong rating in value in MAF V might not be evaluated at the same rating in MAF VI and resulting overall ratings could be lower.

The three lines of evidence for Information Technology are composed of the following:

- Leadership - considers the participation of the senior Information Technology official and their management team, horizontally across government and the span of control for Information Technology within the organization. Most organizations are well established in this area. Leadership will continue to evolve and form an important aspect of the MAF VII assessment.

- Planning - considers the content of the Information Technology plan, related planning and governance processes and how those Information Technology investments are managed through governance structures. Many organizations are in the developmental or formative stages of integrated planning and require more guidance, which will be addressed before the next MAF. Planning will continue to evolve and form a critical aspect of the MAF VII assessment.

- Value - considers the use and plans for use of common and shared services where the Information Technology Shared Service Organization of PWGSC can be the service provider. Management practices for Information Technology service costing, asset management, performance measurement and performance reporting also form part of the assessment. Most organizations are still immature in this area and guidance is required on Key Performance Indicators for Information Technology and good management practices. This will be addressed before the next MAF. Delivering value will continue to evolve and form a critical aspect of MAF VII assessment.

The overall rating for the effective management of information technology for this organization is:

Attention required - The management of information technology is inadequate or ineffective in the areas of leadership, planning or delivery of value from information technology investments. As a consequence, information technology makes an uncertain contribution to the organization's business strategy.

Document overview

Purpose of the IT Plan

The purpose of CEAA Information Services Group IT Plan is to clearly lay out the objectives, strategies, initiatives, performance measures, targets, investments and financials, human resources, and underpinning commitments the CEAA Information Services Group will undertake over the next five years.

The plan will also incorporate the strategies related to the development of the governance processes required in order to meet strategic outcomes in direct support of the CEAA's Agency priorities.

To help CEAA Information Services Group delivering on its accountabilities and its contribution to the achievement of CEAA's strategic outcomes, the CEAA Information Services Group management has recognized the need for an IT Plan to serve as a critical, foundational component of its value stream and management toolkit. The need was also highlighted in MAF Round VI (FY 2008-2009) as an area with attention required.

Creating the plan using TBS Model Plan and Guides assisted us in the assessment of which key areas we needed to focus on, particularly given that we are embarking on the first steps of a five year journey.

This version 1.0 of our plan, emphasis is placed on the business context, CEAA Agency organization alignment and the strategic framework for performance measurements to help drive home the alignment of our strategic outcomes and objectives.

Even thought the Information Services Group has responsibilities on Information Management, this document is specifically for the corporate strategic planning of Information Technology activities. For strategic planning of Information Management, the readers should refer to RDIMS document number: 55603.

Document Structure

This Plan leverages the TBS IT Plan Model and development guidelines related to the Business Context, IT Needs, Governance, Human Resources, Financials, Performance Management and Risk Management.

Please note that some of the sections of the plan and supporting appendices will evolve as CEAA Information Services Group integrated planning and governance processes mature.

Methodology

This plan was conducted with an approach using focused interviews and documentary analysis, not direct observations. In conducting the plan I interviewed managers, and information technology professionals to learn how the organization measured and managed the contribution of information technology towards organizational goals. Interview information was supplemented by documentary analysis.

For quality assurance, my manager and I conducted weekly meetings to review the plan and to add comments. I also distributed the draft copies of the plan to other experts on information technology, evaluation and performance management, and human resource management.

1. Introduction

1.1. CEAA Raison d'être

The Canadian Environmental Assessment Agency (the Agency) provides leadership and serves as the centre of expertise for federal environmental assessment. The Agency works to provide Canadians with high-quality environmental assessments that contribute to informed decision making in support of sustainable development.

1.2. CEAA Responsibilities

Led by the President, who reports directly to the Minister of the Environment, the Agency delivers its mandate under the authority of the *Canadian Environmental Assessment Act* (the Act) and its accompanying regulations and within the framework of the following instruments:

- *The* Canada-Wide Accord on Environmental Harmonization, including the *Sub-Agreement on Environmental Assessment*, and bilateral agreements with provincial governments that establish arrangements for cooperative environmental assessments; and
- International agreements containing environmental assessment provisions to which Canada is a party, principally the United Nations Economic Commission for Europe's *Convention on Environmental Impact Assessment in a Transboundary Context*.

The Agency works with federal authorities on the application of the *Cabinet Directive on Implementing the Canadian Environmental Assessment Act* and its Memorandum of Understanding. The Agency provides advice and guidance on the Directive's expectations and leads interdepartmental efforts to advance the

Directive's goal of delivering high-quality environmental assessments in a predictable, certain, and timely manner.

The Agency is responsible for managing the federal environmental assessment process for most major resource projects and for integrating the Government of Canada's Aboriginal engagement and consultation activities into the environmental assessment process

1.3. CEAA Strategic outcomes

The **CEAA Report on Plans and Priorities 2009-2010 (RPP)**[1] provides an integrated overview of the Agency's Strategic Outcomes, priorities, and expected performance objectives. It also articulates the strategic direction and planning framework needed to ensure we achieve the following **Strategic Outcome**:

> **Environmental considerations are taken into account in federal government decisions respecting policies, plans, programs and projects.**

For this Strategic Outcome, there are a number of program activities, and sub activities, as identified in the department's Program Activity Architecture (PAA), that frame the business lines of the department. These program activities directly contribute to the Strategic Outcome of the department, and are the means by which the department achieves it outcome.

1.4. CEAA Priorities

The departmental Program Priorities, in contrast, articulate where the department intends to focus its efforts. In effect, within each program activity, initiatives and activities will be assessed, and approvals provided, based on how they address these priorities. It is important to note that the priorities complement one or more of the Strategic Outcome.

The Agency has three priorities over this planning period:

- **Build a framework for more integrated environmental assessment;**
- **Play an active leadership role in federal environmental assessment and;**
- **Build the capacity and organization to deliver on existing and new responsibilities.**

[1] http://www.tbs-sct.gc.ca/rpp/2009-2010/inst/eaa/eaa00-eng.asp

1.5. Information Services Group within CEAA organization

The Canadian Environmental Assessment Agency (CEAA) is a relatively small department headquartered in Ottawa. The Information Services Group is one of the divisions found within CEAA. The manager reports directly to the Director General (DG) of Corporate Services sector.

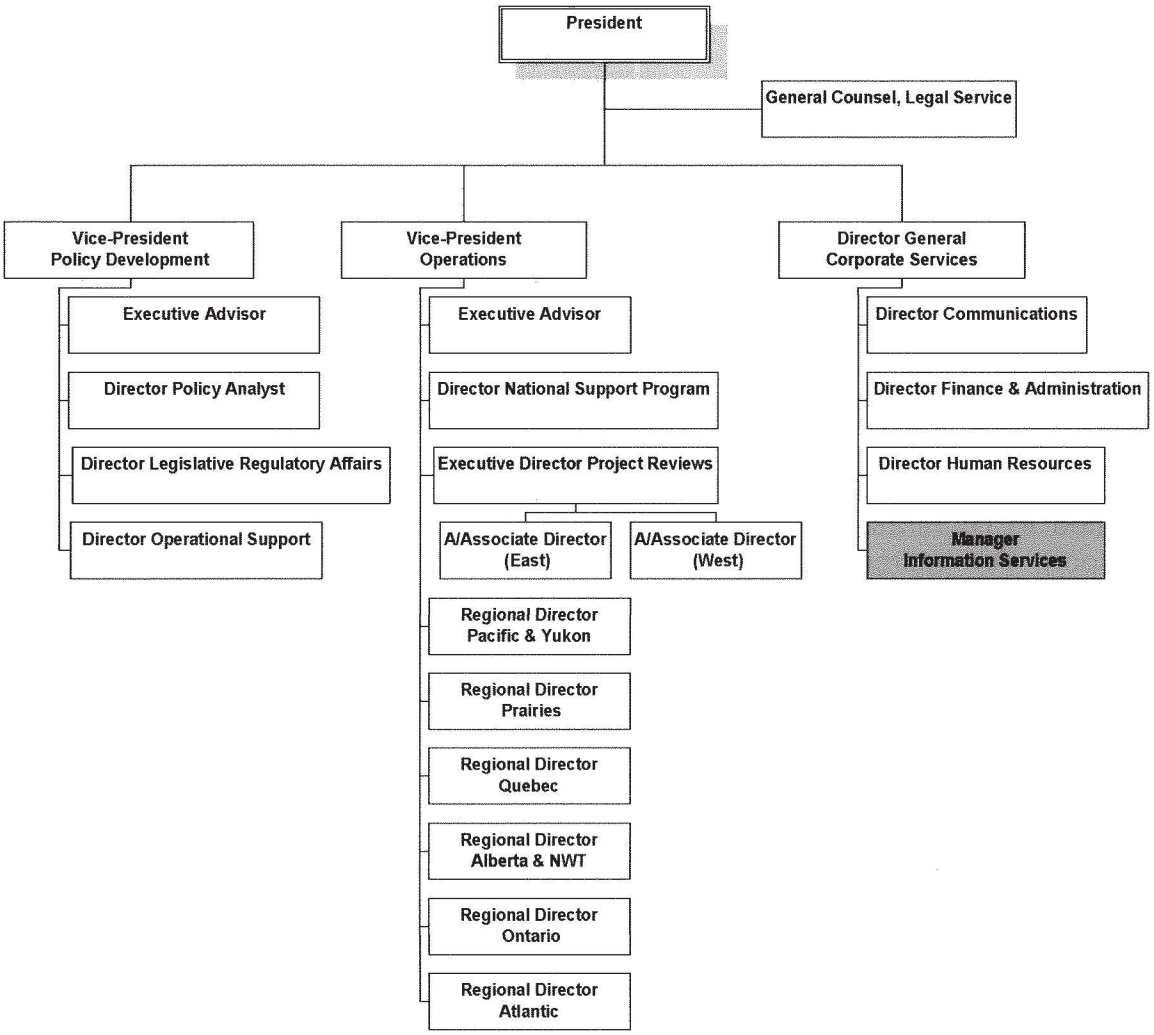

Figure 1: CEAA Organizational chart

The delivery of departmental IM and IT services has changed over the last years since the amalgamation of both services into a single organization, the Information Services (IM&IT) Group staff relies heavily on the IT and IM tools presently in place to support program delivery and reporting needs.

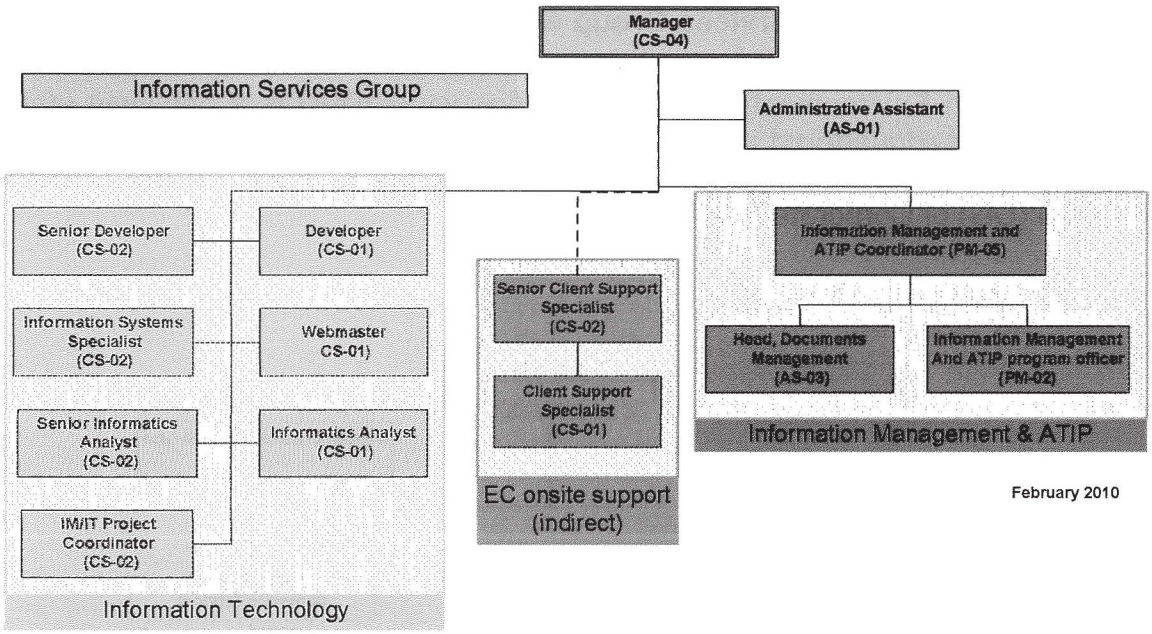

Figure 2: Information Services Organizational chart

The Information Services Group, when fully staffed, is composed of a total of 12 professionals, including the manager. The Information Services Group is divided into 2 sub-groups (see figure 2 above). The IT group's main responsibilities are related to IT infrastructure, architecture as well as application development & support. An Indirect supervision of EC staff that are co-located on CEAA premises to provide desktop-network support to end users. The IM group primaries duties are: records management, information management and ATIP.

2. CEAA IS Division Business

2.1 Vision

The vision of the CEAA Information Services Group Branch is to be a customer-focused, cost-effective, well-run IM/IT operation that is recognized for its responsiveness, flexibility, and the effectiveness of the solutions it provides and supports.

2.2 Mission

The mission of the Information Services Group sector is to provide responsive, quality, and cost-effective information technology solutions and services that enable CEAA's divisions and Regional Offices (RO) to be successful in achieving their respective missions, striving always to exceed expectations.

2.3 Mandate

The Information Services Group is accountable for leading and managing the development and implementation of the corporate vision, strategies, policies, standards and protocols for the management and enhancement of informatics technologies (both Information Management and Information Technology) and related processes across the Agency. It has direct responsibility for all Information Management and Information Technology throughout CEAA, and ensures that department-wide applications, architecture, standards, policies, processes and infrastructure are developed, implemented and enforced.

Business areas for which the sector is responsible include:

IT group:

- **Applications development & support**
- **Architecture** (in coordination with the SLA with EC, see Appendix 1)
- **Infrastructure** (in coordination with the SLA with EC, see Appendix 1)
- **IT Asset management** (in coordination with CEAA's Administration group, see section 3.4)
- **SLA management**
- **Web** (in coordination with the SLA with EC, see Appendix 1)

Information management & ATIP group:

- **Records management**
- **Information Management**
- **ATIP**

2.4 Goals

In addition to the mission statement, mandate, and vision, there are several goals principles that we use in Information Services Group to provide daily direction and focus:

- Provide leadership to CEAA in applying technology to the challenges;

- Provide a full range of application services, including consulting, project management, and business process analysis / re-engineering.

- Provide a robust and flexible computing infrastructure that is capable of handling current and projected needs of internal customers.

- Provide responsive and cost-effective support of installed applications, services, and hardware.

2.5. Objectives

The objective of the Information Services Group is to provide effective, efficient and consistent levels of IM & IT services to all areas of program delivery across the Agency and to further develop the capacity to provide the coherent, authoritative and trusted information systems needed to achieve government and departmental objectives.

Information management and information technology are key enablers of CEAA Program Activities both in terms of providing strategic advice and leadership, innovation, services and technology.

This is reflected in the in the following manner:

- Across all Strategic Outcome areas, through the provision of basic infrastructure and support to "general-use" software applications (e.g. e-mail, office application suites, corporate finance, human resource applications and information management).

- Within specific Strategic Outcome areas, through the provision of specialized hardware infrastructure in support of Program Activities, through the provision of services in support of these activities (including development, implementation and maintenance of specialized application software for the collection, storage, analysis and dissemination of environmental data and products), and, through data and information management services.

Management efforts in the IT domains are directed towards ensuring alignment of IT resources and services with departmental priorities such that the best outcomes are achieved by using existing resources and infrastructure where possible, and making strategic investments in evolving technologies and capacity as required.

2.6 Alignment with Shared Services and Other Related IT Initiatives

Shared services are viewed as a way of producing more effective, efficient and economical delivery of common services within and across government departments. CEAA has developed a partnership with Environment Canada (EC) for IT shared services through a Service Level Agreement (SLA)[2]. This initiative is aligning with Treasury Board of Canada Secretariat-led Corporate and Administrative Shared Services (CASS) initiative.

[2] InfoZone #:

As part of that initiative, CEAA has factored a number of departmental and government-wide initiatives into its five year plan.

Key among these includes the following:

- Citizen-Centered Service Delivery (ensure CLF 2.0 compliance);
- Management of Information Technology Security (MITS);
- Adoption of Government-Wide Common and Shared Services;
- Alignment to the IM & IT Organizational Readiness Office (ORO) Initiative;
- Integrated Investment Planning.

The IT Plan is referenced as one of the sources providing more details how initiatives contribute to excellence. This inclusion is a strong demonstration of Information Management and Technology (IMT) alignment to the business.

The disciplines of Information Management (IM) and Information Technology (IT) are converged in CEAA based on the premise that IT enables IM, and must be addressed together to ensure performance objectives are achieved, and effective.

The Agency's Corporate Business Plan will recognize the IT Plan as a key artefact contributing to management priorities. Specifically, the Information Services Group continues its commitment to both Service Level Agreement and the Information Management Agenda (with a focus on Electronic Document and Records Management this year). These two significant initiatives directly support the Agency in its due diligence, management, results reporting, and proactive disclosure of information.

3. Governance

3.1 CEAA Governance (Decision Making Process)

Both the Agency Executive Committee (AEC) and Operations Committee (OPS) are responsible for overall strategic direction and management of the department. There also is a series of other committees charged with specific components of the department's planning, policy, reporting and evaluation responsibilities. The AEC and OPS committee is composed of senior management of all divisions within CEAA.

At all levels of the organization, strategies are governed by the following principles:

- All planning activities are framed by the departmental Strategic Outcomes.

- All plans and activities are informed by risk assessment/management strategies.
- All plans are informed by, and responsive to, the results achieved and reporting on in the previous reporting period.

The Regional Offices within the department are critical in ensuring CEAA achieves its objectives and outcomes. Each region is led by a Regional director, who is responsible for ensuring the region responds and achieves the desired outcomes of the department.

3.2 CEAA Information Services Group Governance (Decision Making Process)

The approach of CEAA Information Services Group governance ensures alignment with the business. The IT manager works in collaboration with business clients. IT Business and Operational decisions are made by the IT manager, who ensures due diligence and justification are provided for any procurement or maintenance requirements. The IT manager is accountable to the Director General of the Corporate Services.

3.3 Opportunity Assessment & Priority Setting

The Agency overall approach to strategic planning is to identify key challenges and risks, assess the performance measurement framework, review of human resources issues, and then to review priorities and projects. The following chart represents the CEAA's approach of strategic priority planning.

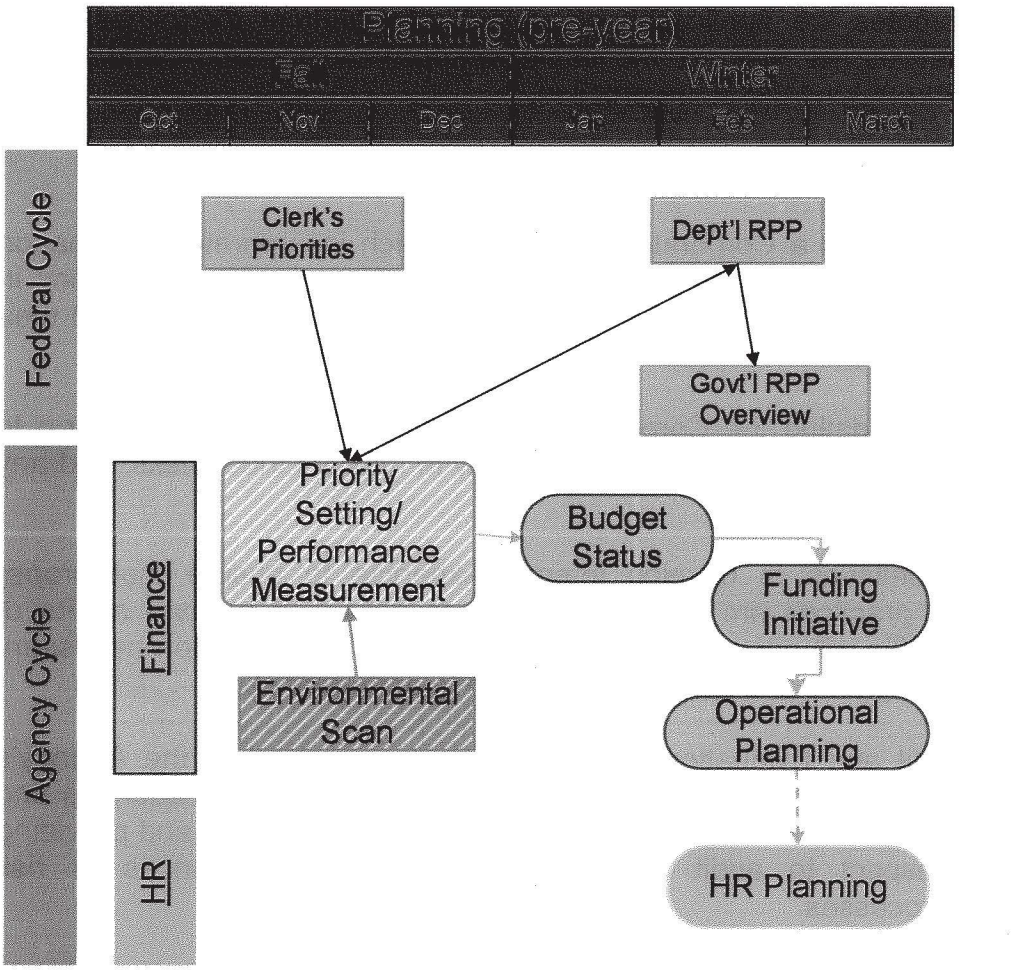

Figure 3: CEAA planning cycle

3.4 Portfolio Management Approach for Oversight & Reporting

To deliver IT services effectively, the CEAA Information Services Group must maintain alignment of resources with departmental priorities. The CEAA Information Services division will develop, over the next fiscal year; a portfolio management approach to ensure effective communication at all levels and thus create closer ties with others division in CEAA.

CEAA Information Services Group will use the Enhanced Management Framework (EMF)[3] from TB of Canada. The EMF focuses on two broad areas: portfolio management and project management. It stresses the importance of aligning business planning with an integrated IT strategy. This strategy should set priorities and budgets for the organization's IM and IT investments, allowing it to assess and successfully manage projects, existing operations, enhancements and innovative pathfinders.

[3] http://www.tbs-sct.gc.ca/emf-cag/abu-ans/abu-ans-eng.asp

EMF also promotes the application of project management disciplines to all approved initiatives, as well as the implementation of risk and performance management throughout the entire process.

3.5 Risk Management

The Agency maintains a Corporate Risk Profile which incorporates information collected at both the corporate and operational levels to assist the Agency in understanding the range of risks it faces, their likelihood of occurrence and their potential impacts.

Developing and updating the Corporate Risk Profile allows the organization to evaluate its risk tolerance, its ability and capacity to mitigate those risks, and any learning needs.

The Agency continues to develop internal expertise to ensure that proper processes and practices are in place to assess risks and perform audits of priority areas. This will ensure that management has the information necessary to evaluate its programs and take steps to improve performance.

An internal Audit and Evaluation Oversight Board comprised of the Agency's senior executives has been established to provide the necessary leadership and accountability. The Board acts in an advisory capacity, monitoring and providing advice with respect to audit and evaluation, including advances in risk management processes.

Both IT & IM strategic operations are supported by risk management strategies consistent with the Agency approaches. From a strategic perspective, IT management or his delegation of authority's participation on the Corporate Planning Committee, with review of the Corporate Risk Profile, enables IT to define mitigation strategies in the form of possible solutions and initiatives.

CEAA Information Services Group will improve his IM & IT project level management by embedding risk management into his IT portfolio management approach.

4. Finance

4.1 Funding

The Information Services Group budget funding comes from the recurrent allocation budget of the Corporate Services sector.

4.2 Budget Allocation

As illustrated in the table below, the budget allocation of the Information Services Group in FY 2009-2010.

Financial Code	Description	Amount ($)
40000	IT Salary	$433,246
40000	IM Salary	$277,345
44500	O&M IT	$1,039,196
44500	O&M IM	$213,000
	Total	$1,962,787

Table 1: Budget Allocation

O&M costs are explained more in details in section 4.4. Efficiency opportunities will be undertaken where time and resources permit, for further IT effectiveness and efficiency improvements and/or cost savings.

4.3 Projection over the next 5 years

This projection for the next five years is based on keys assumptions from the previous years and corporate planning budget. We anticipate that salary, O&M and SLA costs will grow by 3%.

5 years Projection				
FY 2009-2010	**FY 2010-2011**	**FY 2011-2012**	**FY 2012-2013**	**FY 2013-2014**
$1,962,787	$2,021,671	$2,082,321	$2,144,790	$2,209,134

Table 2: 5 years budget projection

4.4 Budget by Asset Classes

The following table contains data on the FY 2009-2010 estimated non-salary IT & IM resources:

Financial Code	Description	Amount ($)
40000	General Operations, supplies and IM/IT Community	$10,000
40000	General (IM)	$10,000
40000	ATIP Professional Services Contract (IM)	$50,000
40001	Learning activities	$8,000
40001	Learning Activities (IM)	$3,000.
44501	IT Service Level Agreement with EC	$694,196
44504	Web Site and Web Application Development	$100,000
44504	IM Systems project support and	$70,000

	maintenance	
44504	Ministerial Correspondence	$62,000
44504	Records Room IT Systems	$20,000
44505	Records Room Support (IM)	$15,000
44508	Equipment renewal and maintenance (National)	$75,000
44509	IM Initiatives / Development (IM)	$135,000
	Total	**$1,252,196**

Table 3: Budget by Asset Classes

4.5 Costs per IT Service

As CEAA Information Services Group evolves it will continue to evaluate and adapt various IT service delivery models, processes and best practices to suit its needs. Service Level Agreement(s) or Memorandum of Understanding will be reviewed annually or when a new service or product is required.

This table show the IT services cost cover by the Service Level Agreement[4] with EC.

Service Name	**FY 2010/2011**
Fundamental services (include support/basic & Desktop/Helpdesk & Security services)	$439,917
IT Central Fund	$86,000
Applications, development & maintenance services	$40,882
Server Support services	$20,790
Database hosting services	$8,190
Web hosting services	$16,700
Telecommunications (Videoconferencing services)	$232,320
Blackberry services	$14,868
Correspondence tracking - CCMMercury	$684
Total	**860,411.00$**

Table 4: Cost per IT Services

4.5 Life-cycle Management (Total Cost of Ownership)

CEAA's Administration group & Information Services group manage the IT assets life cycle. Each group has different responsibilities depending on the nature of the IT assets.

[4] InfoZone #

Information Services is responsible for the software & licensing products, on the other hand the Administration group is responsible for hardware type of IT assets.

In coordination with Environment Canada through a Service Level Agreement, CEAA's Information Services Group manages all core systems, software packages and licensing.

All products have been assessed and are:

- Products are essential to the CEAA mission
- Products are widely used across the main CEAA offices
- Sufficient support resources exist
- Valid licenses exist
- Standard

CEAA's Administration group is committed to plan an Investment Planning process that prioritizes IT hardware asset investment requirements and assess risk. Investment planning is a comprehensive process that incorporates principles, tools, and senior management oversight and ensures investment strategies and plans are developed departmentally across all asset categories.

Using a planning process[5], Administrative Group's focus is to prioritize and fund lifecycle management requirements to maximize reinvestment into the existing IT asset base.

CEAA Administrative Group has developed a plan that references planned IT investments over the next years in support of departmental outcomes and will have the objective of obtaining adequate resources to sustain the CEAA's IT assets.

All IT assets are being authorized by Information Services & Administration Groups managers and procured through contracting processes to ensure that all IT assets acquired are effectively tracked from the moment of acquisition through to the end of their useful life and that they conform to the Agency standards.

See Appendix 2 for IT assets inventory

4.6 Resource Planning Details (Per Project)

The Information Services Division has a significant allocation under Business Application; this includes funding for contract engagements and key commitments to the following for the next fiscal year (FY2010-2011):

- **Electronic Document and Records Management (InfoZONE)**

[5] Need input from Stéphane

- **IM & IT Security policy implementation**
- **Project Repository application**
- **Phoenix application**

A summary of the planned IM & IT projects over the five year planning cycle is provided in the following table. Differences between available and allocated FTEs are made up with students and temporary help.

Project	Start Year	Project Phase as of March 2010	Resources allocated (FTEs)
Electronic Document and Records Management	2009	Implementation	3.5
CEAR	2000	Maintenance & Support	1.5
Project Repository application	2009	Maintenance & Support	1.5
Phoenix application	2009	Assessment	.25
Gis web application	2009	Maintenance & Support	.5
UM application	2008	Maintenance & Support	.25
IAM application	2005	Maintenance & Support	.25
Online Registration application	2009	Maintenance & Support	.25
IM & IT Security policy implementation	2010	Assessment	.5
IT Management	2010	Assessment	1.0
Web	2000	Maintenance & Support	1
Administration	Ongoing	Ongoing	2.0
		Total	**12.5**

Table 5: Planned Projects

5. Human Resources

5.1 Resource Allocation

Information Management and Technology services are provided by 12 IT professionals at CEAA Headquarters Information Services division, reporting through one manager, who is accountable to the Corporate Services Branch. Business Function Inventory is summarized as follows:

- Information Management
- Infrastructure/Architecture/Asset Management.
- Application/Projects Management.
- Web Management

Level	Title	FTEs
CS-04	Manager	1.0
AS-01	Administrative assistant	1.0
	IT	
CS-02	Project coordinator (proposed)	1.0
CS-02	Systems Analyst	1.0
CS-02	Information Systems Analyst	1.0
CS-02	Information Systems Analyst	1.0
CS-01	Informatics Analyst	1.0
CS-01	Informatics Analyst	1.0
CS-01	Web site officer	1.0
	IM	
PM-05	Coordinator of ATIP and IM	1.0
PM-02	ATIP officer	1.0
AS-03	Head document management	1.0
	Total	**12.0**

Table 6: Resources Allocation

5.2 IT Competencies / Skills Inventory / Career Path

Information Services division has undergone change this year and has been rebuilding along with moving forward with key commitments and implementing new technologies. As such, consideration of our competencies is crucial as we build for the future.

Section	Level	Title	Role	Skills
Manager Office	CS-04	Manager	Management	-Policy planning -Strategic planning -Management processes -Business Analysis -Projects / portfolio management

				-IT asset management
	AS-01	Administrative assistant	Administrative support	-Management processes -Administrative support
IT section	CS-02	Project coordinator (proposed)	Coordinator & analyst	-Projects / portfolio management -Business Analysis
	CS-02	Systems Analyst	Server/Network Analyst	-Architecture & Infrastructure management -Business Analysis -Security Analysis
	CS-02	Information Systems Analyst	Programmer Analyst	-Database design & management -Application Development & support -Business Analyst
	CS-02	Information Systems Analyst	Programmer Analyst	-Database design & management -Application Development & support -Business Analyst
	CS-01	Informatics Analyst	Programmer Analyst	-Database design & management -Application Development & support -Business Analyst
	CS-01	Informatics Analyst	Server/Network Analyst	Architecture/Infrastructure management -Business Analysis -Security Analysis
	CS-01	Web site officer	Webmaster	-Web site design & support -Web site management
IM section	PM-05	Coordinator of ATIP and IM	Coordinator & analyst	-Supervision -Management of processes and products to support ATIP & Information management
	PM-02	ATIP officer	ATIP analyst	-Analyzing documents for disclosure in accordance with the ATIP legislation.
	AS-03	Head document management	IM support	-Management of records information -Support and advice on information management

Table 7: Employees skills

6. PERFORMANCE MEASUREMENT

Governance-focused IT departments use IT performance management approaches to improve their understanding of what the business wants from IT and consequently what IT has to deliver.

The basic purpose of any measurement system is to provide feedback, relative to your goals, that increases your chances of achieving these goals efficiently and effectively. Measurement gains true value when used as the basis for timely decisions.

If you can't measure it, you can't manage it. Credible business measures of IT effectiveness are essential to all levels of business planning and prioritizing the use of IT.

6.1 Outcomes

In direct support of the strategic maps, outcomes and initiatives, CEAA IS division must & will develop performance management measures and targets. We will measure our IT dimensions: financial, human resources, learning, operational processes.

6.2 Performance Measurement, Reporting & KPIs

As a small department, CEAA IS division will measure several Key Performance Indicators (KPIs), adapted from TBS best practices.

The following table provides our planned KPIs for the upcoming fiscal years. As we improve and refine our IT governance management these KPIs could change over the years.

Performance Measurement				
Objectives	**Description**	**KPI Indicator**	**Target**	**Frequency**
Finance				
Budget alignment	Good management of IT&IM budget allocation	$ in deficit or surplus	Zero deficit	Quarterly basis
Human Resources				
Attract & retain IT personnel	Vacant permanent position	Number of vacant permanent position	0	Quarterly basis
Internal Processes, Services & Projects				
IT strategic	Linkage of	Completion of	Approbation	Annual

alignment	business and IT activities with corporate objectives	an IT plan & IT plan annual review	of IT plan or its annual review by end of FY 2010-2011	basis
IT Portfolio management	Implementation portfolio management	Completion of portfolio management Implementation	Successful implementation by end of FY 2010-2011	Quarterly basis
IT & IM Security Policies	Development of IT & IM Security Policies	Completion of IT & IM Security Policies Implementation	Successful implementation by end of FY 2010-2011	Quarterly basis
SLA monitoring	Monitoring of services provided & planned costs	Number of meetings with EC's management	4 meetings by end FY 2010-2011	Quarterly basis
InfoZONE (EDIMS)	Implementation of electronic document information management system	Completion of electronic document information management system Implementation	Successful implementation by end of FY 2010-2011	Monthly basis
Projects/ Applications delivery	Projects/Applications delivery on time and within budget	% of projects that are executed in the planned time-frame and budget (costs) based on their baseline	100%	Quarterly basis
Helpdesk Support	Number of calls received and closed	% of Number of calls received and closed within a month	100%	Monthly basis
Web	CLF 2 compliance	% of web pages in compliance with CLF2	100% by end FY 2010-2011	Quarterly basis

		standards		
Network Security Breaches	Monitoring of network security in coordination with EC	Number security breaches	0 (target level in SLA)	Monthly basis
Expected Network Uptime	Monitoring of network in coordination with EC	% of uptime	99% (target level in SLA)	Monthly basis
Learning & Growth				
IT staff competencies	All staff annual learning commitments	% of completion	100% by end FY 2010-2011	Quarterly basis
IT staff competencies	Agency mandatory training courses	% of completion	100% by end FY 2010-2011	Quarterly basis

Table 8: Performance measurements

7. Security

The Policy on Government Security (PGS) states requirements for protecting government assets, including information, and directs the federal departments and agencies to which it applies to have an IM and IT security strategy. The Policy on the Management of Government Information requires that departments protect information throughout its life cycle.

The introduction of the Operational Security Standard (OPS): Management of Information Technology Security (MITS) compels all federal departments and agencies to develop an IM and IT security management strategy and implement it within timeframes established by the Treasury Board Secretariat.

IT & IM related security is managed within the Information Services Group. CEAA IS group is committed to the Policy on Government Security (PGS) and related Operational Security Standards (OPS). In Addition CEAA IS group will conduct its security program in order to support the CEAA in achieving its strategic outcomes.

In support of the GSP, and in conjunction with CEAA Administration Unit, the Information Services Group has lead responsibilities to:

- Ensure the confidentiality, integrity and availability of the Agency's use of our Service Provider's(Environment Canada (EC)) network, by:
    - Implementing the requirements of the Management of Information Technology Security (MITS) Operational Standard.
    - Developing and publishing IT security policies, directives and guidelines.

  - Reviewing and approving IT threat and risk assessments.
  - Monitoring, reviewing and controlling access to Agency audit trails.
  - Coordination between the Agency and EC for Conducting Electronic Networks Content Monitoring.
  - Developing and managing a comprehensive IT Security Awareness Program, in cooperation with the DSO.

- Ensure the confidentiality, integrity and availability of CEAA information, by:
  - Developing and publishing the Information Security Directive.
  - Developing directives and guidelines for the marking, handling, storing, transmitting and destruction of sensitive information and assets, in order to ensure the confidentiality, availability and integrity of corporate information.
  - Supporting the cost-effective implementation of appropriate IM/IT security measures at the CEAA.

In order to enable risk tolerable execution of CEAA departments' initiatives and programs, CEAA IS group will develop an IM and IT security policy in the next fiscal year.

In addition, as mentioned in our Service Level Agreement (SLA)[6] with Environment Canada (EC), implements the following security:

- All systems are secured to "Protected A" designation. A protected A designation
- Anti-virus - McAfee suite of products is currently used to protect the desktop.
- Patch management tools are used to automatically update vulnerable systems and desktops in the light of a potential threat or an on-going attack.
- File filtering of email attachments: Antigen is the product used on Exchange servers to filter file types of email attachments and to delete those suspecting of carrying malicious codes.
- Anti-spam tool: all necessary measures are taken to reduce and potentially eliminate the reception of "junk mail" including pornography with the help of a filtering tool.
- Accounts - All users must have a username and password to access systems and services. Passwords are set to expire periodically.
- Remote Access - Users must be registered with the secure access server in Dorval. This is accomplished when they are given remote access

[6] See Appendix 1

services. All remote access through dial-up is protected by username and "one-time" password.

- External networks - Unauthorized intrusion from GENET and Internet is screened by a firewall at TLC.
- Physical Access - Access to critical NCR infrastructure components is highly restricted. Computer rooms and communications closets are locked. Access to main computer areas is monitored and logged with an ADT security system.

Systems integrity and user data integrity is preserved by performing regular maintenance and through the creation of backup tapes of all private and shared resources. The following backup procedure is adhered to:

- Files on servers are backed up on to tape on a regular basis.
- The frequency (daily, weekly, monthly) and type (full, differential, incremental) is dependent upon the type of server, the volatility of the data etc. In general, files that have been created or modified are backed up each day.
- Backup tapes are sent off site, to guard against a catastrophic event. These tapes would be used to rebuild servers in the event that a catastrophe occurred that destroyed everything in the computer room.
- Backup tapes are kept for varying amounts of time for as long as 1 year.
- CEAA (through a Service Level Agreement with Environment Canada), with the help of the Secure Applications and Key Management Services (SAKMS) from Public Works Government Service Canada (PWGSC), provides digital certificates for the transmission of email suitable for handling information up to Protected B

8. Information Management

The information management (IM) team has been going through significant change and continues its responsiveness to clients and delivery of services as planned. The information management strategy was presented earlier this year with an update of the IM Vision.

The Agency is looking to implement Information Management systems to meet many of its objectives. These are outlined in the Information Management 5 Year Strategic Plan[7]. The objectives are listed as:

- Use of a single managed information repository

[7] CEAA IM Strategic Plan 2009-2014, RDIMS 55603

- Standardization of processes with policies that support use of IM techniques
- Implementation a meta data management framework
- Development of a consistent governance approach to IM
- IM becomes a key enabler of Agency processes
- Promote environmentally conscience practices
- Fulfillment of all IM-related legal and policy requirements within the Government of Canada

Even thought the Information Services Division has responsibilities on Information Management, this document is specifically for the corporate strategic planning of Information Technology activities. For strategic planning of Information Management, the readers should refer to CEAA IM Strategic Plan 2009-2014 RDIMS document number: 55603.

9. Accessibility

The Information Services Group, along with Communication Group, has made a significant effort last year (2009) to be compliant with Treasury Board of Canada (TBS) Common Look and Feel 2 (CLF2) principles. These guidelines imply standards on web addresses, web accessibility, web pages formats and emails. The Agency score department on TBS CLF assessment reporting 2009/10 was 96%[8]. The Information Services Group is committed to improve Agency's web sites accessibility where areas of improvements have been identified in the TBS assessment report.

10. Action

This IT Plan will continue to evolve to meet the Agency's requirements, and will be driven by CEAA's business direction, priorities and levels of investment. This plan does not seek to prescribe solutions, but to provide structure and direction for effective and collaborative planning and implementation.

As the Information Services Group moves forward, it will continue to revise the criteria by which priorities will be set, and undertake ongoing monitoring of progress.

10.1 Implementation

Following are Information Services Group's key commitments for fiscal year:

1. **IT Governance management implementation**
   Fundamentally, IT governance is concerned about two things: IT's delivery of value to the business and mitigation of IT risks. The first is driven by strategic

[8] Common Look and Feel V2 Compliancy Audit (EDRIM # 55156)

alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained.

This leads to the five main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk management. Three of them are drivers: strategic alignment, resource management (which overlays them all) and performance measurement.

The following steps are scheduled[9]:

1. **Set up a governance organizational framework.**
That will take IT governance forward and own it as an initiative, with clear responsibilities and objectives and participation from all interested parties.

2. **Align IT strategy with business goals**.
What are the current business concerns and issues where IT has a significant influence? Identify the top IT issues on management's agenda.

3. **Understand/define the risks**.
Given top management's business concerns, what are the risk indicators relating to IT's ability to deliver against these concerns

4. **Define target areas.**
Identify the process areas in IT that are critical to managing these risk areas.

5. **Analyze current capability and identify gaps.**
Perform a capability assessment to find out where improvements are needed most.

6. **Develop improvement strategies.**
Decide which are the highest priority projects that will help improve the management and governance of these significant areas. This decision should be based on most potential benefit and ease of implementation, and a focus on important IT processes and core competencies.

7. **Measure results.**
Establish a balanced scorecard mechanism for measuring current performance.

2. Information Management systems implementation

The Canadian Environmental Assessment Agency currently lacks a unified system and standards to effectively manage the information that it must process.

[9] *www.itgi.org* and *www.isaca.org*

There are a series of activities that will enable the Agency to meet its requirements that can be mapped out into distinct phases. Each of these phases must be aligned with the strategic goals, which are in turn aligned to the Agency's priorities and mandate. These goals and actions should be viewed as an evolving list, as the development of an effective IM system will constantly evolve to meet the Agency's needs. The strategy will be reviewed yearly, and re-aligned as necessary.

The following steps are scheduled:

- Development and approval of an IM Strategy
- Development and approval of IM Policies and Guidelines
- Establish Meta Data Standards
- Implement new internal IM System into production
- Implement new external IM system (CEAA & Partners)
- Migrate existing RDIMS to new IM System and de-commission old infrastructure
- Migrate legacy systems (e.g. REAC sites to new external IM solution)
- Produce and deliver training material to all users
- Development and implementation of the Project Repository version 2, along with enhancements
- Maintenance of CEAR as well as other applications

3. IT & IM Security policy implementation

Management of all IM and IT Security issues is the overall responsibility of the Information Services however, other key participants such as Environment Canada (through a Service Level Agreement with Environment Canada) National IM and IT Security Coordinator (NIMITSC); plays a strong role as we use their IT infrastructure.

The following steps are scheduled:

- Be involved in the IM & IT Security Program management of EC. e.g. CEAA should be represented in NIMITSC;
- Develop and promote IM and IT Security policies;
- Share information related to an evolving IT environment;
- Review proposed changes to the IT infrastructure and assess impact on security controls;
- Monitor and respond to an ever-changing threat environment;
- Recommend additional controls based on increased risks;
- Provide security guidance to major IT projects;

- Develop and implement a prioritized list of information systems for Certification and Accreditation (C&A);
- Identify minimum C&A deliverables to system leads, including guidance on developing the deliverables;
- Recommend information systems for Accreditation to their Accreditation Authority; and,
- Develop and promote IM and IT Security awareness.

10.2 Capacity & Sustainability Assessment

CEAA Information Services Group must provide the necessary applications and infrastructure to the Agency and ensure that they are sustainable, now and in the future. CEAA Information Services Group capability and discipline in the area of sustainability and capability assessments will continue to mature over time, as certain assessments are operationally driven while others are investment, initiative and/or project specific. In the next fiscal year (FY2010-2011), the establishment of our governance and portfolio/project management framework and related processes are expected to further enhance the Information Services Group's capabilities in this area overtime.

10.3 Risk Management

This table show the identified IM & IT risks areas from the Corporate Risk Plan for the fiscal year 2010-2011:[10]

Risk Areas	Likelihood (Low, Med, High)	Impact (Low, Med, High)
Information Technology		
Canadian Environmental Assessment Registry Internet Site (data integrity) Risk of non-compliance with the Canadian Environmental Assessment Act and relevant legislation	Med	Med
Canadian Environmental Assessment Registry Internet Site (system integrity) Risk of system failure	Low	High
Service Level Agreement Risk of not obtaining required Information Technology Services from Environment Canada	Low	Low
Knowledge Management Risk of loss of knowledge/information due to expansion of the organization and	High	High

10

employee turnover Risk policies/guidelines are not developed and transferred in a timely manner		
Information Management		
EDIMS (InfoZONE) *IM/IT no records management system, ATIP, registry and litigation very difficult and time consuming to respond to*	Med	Med
IM Compliance Risk that information management systems do not adequately support legal challenges of the Act or review processes conducted under them Risk that IM does not adequately support statutory reporting	Med	High

11. Annual Update

An update should be provided for the next fiscal year (FY2011-2012)

The annual update cycle of this IT plan is scheduled to be synchronized with the Agency Corporate planning review in September and fiscal year's end.

Bibliography

Bajjaly, S. T. (1998), *Strategic information systems planning in the public sector*, *The American Review of Public Administration,* 28, 76-86.

Bozeman, B. & Bretschneider, S. (1986), *Public management information systems: Theory and prescription*, Public Administration Review, 46, 475-487.

Caudle, S. L., Gor, W. L. & Newcomer, K. E. (1991), *Key information systems management issues for the public sector*, MIS Quarterly, 15, 171-188.

IT Governance Institute (2003) Board Briefing on IT Governance, 2nd ed. Available online at
www.itgi.org (accessed 22 September 2005).

IT Governance Institute, Enterprise Value Governance of the IT Investment – The Val IT Framework

IT Governance Institute (2005) Governance of the Extended Enterprise: Bridging Business and IT Strategies. Wiley, New Jersey.

Kaplan, Robert S. and Norton, David P. "The Balanced Scorecard -- Measures that Drive Performance," Harvard Business Review, Vol. 70, No. 2 (January-February 1992).

Kaplan, Robert S. and Norton, David P. "Putting the Balanced Scorecard to Work," Harvard Business Review, Vol. 71, No. 5 (September-October 1993).

Kaplan, Robert S. and Norton, David P. "Using the Balanced Scorecard as a Strategic Management System," Harvard Business Review, Vol. 74, No. 1 (January-February 1996).

Public Administration, Volume 85, Issue 3, Page 857-860, Sep 2007.

Society for Information Management Advanced Practices Council. Practitioner's Guide to I. S. Performance Measurement. Chicago: Society for Information Management, March 1995.

Weill, P. and Ross, J.W. (2004) IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press, Boston, Massachusetts.

White, J. D (2007), *Managing Information in the Public Sector*, New York, M. E. Sharpe, 319 p.

Internet

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_IT/pfit-csit01_e.asp

http://www.tbs-sct.gc.ca/maf-crg/indicators-indicateurs/2008/stewardship-gerance/stewardship-gerance-eng.asp

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249&section=text#appB

Treasury Target Performance Architecture Executive Guide: Measuring Performance and Demonstrating Results for Information Technology Investments, http://www.gao.gov/special.pubs/ai98089.pdf

Contributors to This Plan

Richard Gagné
Director of Corporate Services at CEAA

Gilles Lévesque
Manager of Information Services Group at CEAA

Chantal St-Germain
Director, Business Operations at Environment Canada

Janet L. Arnold (to come)
Senior IT Analyst, CIO Branch, IT Division at Treasury Board

Scott Forster
Performance and evaluation officer at CEAA

Yves Dinel
Senior HR advisor at CEAA

Stéphane Parent
Senior administration officer at CEAA

Appendix 1 - Service Level Agreement with EC

1. Introduction

1.1 Agreement Overview

This Agreement represents a Service Level Agreement between the Chief Information Officer Branch (CIOB) of Environment Canada (EC) (hereafter referred as to CIOB EC) and Canadian Environmental Assessment Agency ((hereafter referred as to CEAA or the "Client") for the provision of IT (information technologies) services required to support and sustain CEAA IT services.

The purpose of this agreement is to ensure that the proper elements and commitments are in place to provide consistent IT service to the CEAA by CIOB EC.

To goal of this Agreement is to obtain a mutual agreement between CIOB EC and CEAA.

The objectives in this Agreement are to:

- Provides clear reference to service ownership, accountability, responsibilities and/or roles;
- Present a clear concise and measurable description of service provision to the client;
- Match perceptions of expected services provision with actual service support & delivery.

1.2. Business Contacts

CLIENT CIOB EC

Name	**Gilles Lévesque**	**Name**	**Joanne Racicot**
Title	CEAA Information Services Manager	**Title**	Director, NCR Division, IT Operations & Client Support Directorate
Address	Place Bell Canada 160 Elgin Street, 22nd Floor Ottawa, Ontario K1A 0H3 Canada	**Address**	351 St Joseph Blvd Gatineau, Quebec K1A 0H3 Canada
Phone #	613-957-0356	**Phone #**	819-953-4516
Fax #	613-957-0946	**Fax #**	819-953-4509
E-mail	gilles.levesque@ceaa-acee.gc.ca	**E-mail**	joanne.racicot@ec.gc.ca

1.3 Service Scope

The following services of covered by this agreement:

Line of business	Service Name
Information Services - CEAA	Fundamental services
Information Services - CEAA	Desktop/Helpdesk services
Information Services - CEAA	IT Central Fund
Information Services - CEAA	Application, development services
Information Services - CEAA	Server Support services
Information Services - CEAA	Database hosting services
Information Services - CEAA	Web hosting services
Information Services - CEAA	Videoconferencing services
Information Services - CEAA	Blackberry services
Information Services - CEAA	Correspondence tracking -CCM mercury

Table 1: List of services

1.4 .Exclusion / Limitations

The following are excluded from the service:

- Asset management
- Evergreen life cycle
- Network printing

1.5 Roles & Responsibilities

1.5.1 Client Responsibilities

- Adherence to any related policies, processes and procedures as defined in this SLA;
- Advance scheduling of all service related requests and other special services with CIOB EC;
- Payments of all costs associated with the services defined in section 2 and such as required set-up and/or configuration, prior to the service provision;
- Client availability for problem solving that are related to incident or that required Client support related to service levels;
- Reports all Service related incidents and question to the Service Desk.

1.5.2 CIBO EC Responsibilities

- Provision of proper services in accordance with any related policies, processes and procedures as defined in this SLA;
- Facilitation of all service support activities;

- Provision of appropriate advanced notification.

2. Provision and managing services

The following sections provide relevant details on service availability, monitoring, measurement and reporting of in-scope and related components.

2.1. Hours of service

Coverage parameters specific to the Service(s) covered in this Agreement are as follows:

Services	Normal Hours of services	Hours of support
Fundamental services	24x7	Monday to Friday [11] 7h00am-5h00pm
Desktop/Helpdesk services	24x7	Monday to Friday 7h00am-5h00pm
Application, development & maintenance services	24x7	Monday to Friday 7h00am-5h00pm
Server Support services	24x7	Monday to Friday 7h00am-5h00pm
Database hosting services	24x7	Monday to Friday 7h00am-5h00pm
Web hosting services	24x7	Monday to Friday 7h00am-5h00pm
Telecommunications (Videoconferencing) services	24x7	Monday to Friday 7h00am-5h00pm
Blackberry services	24x7	Monday to Friday 7h00am-5h00pm

Table 2: Hours of services

Service Desk
Phone #: (819) 953-3687
E-mail: Helpdesk@ec.gc.ca

2.1.1 Service Extension Arrangement

The Client can request temporary additional support coverage by contacting CIOB EC. A minimum lead-time of 5 business-days is required. Additional support can be provided at a per client rate as negotiated.

[11] Support for the service In local time

2.2. Service Maintenance & Availability restrictions

Maintenance window timeframe should be during the weekend (e.g. from Saturday 8h00pm to Sunday 9h00am Eastern Time).

These are the times when regularly scheduled maintenance (planned outages) to Services in this SLA and/or its components is performed. These activities may render systems and/or applications unavailable for normal user interaction.

2.3. Service Levels

CIOB EC service level targets 99% services availability. CIOB can meet this objective by providing proactive system monitoring and have the necessary hardware and software maintenance resources to support CEAA needs.

2.4. Service Reporting

CIOB EC will provide an annual report of services performance and availability. CEAA will be able to track ongoing services issues/request via the Service Desk.

2.5. Service Reviews

Meetings between CIOB EC and CEAA will be held on a quarterly basis to review the Services in the last period. All action will be recorded and reviewed at the next service review meeting.

2.6. Service Security

CIOB EC IT Operations takes all reasonable and prudent measures to secure its systems and services and to protect client data. Network security provides a reasonable shield against hostile intrusion.

All CIOB EC systems are secured to "Protected A" designation. A protected A designation means that the unauthorized release of this information could cause injury to an individual, organization or government.

Client should not expect to use EC systems or networks to store or transmit documents that have a higher security designation or classification. All CEAA employees must be aware of and follow the “Use of Electronic Networks Policy”:

Client must implement appropriate safeguards to mitigate application vulnerabilities.

CIOB EC and CEAA mutually agree to adhere to relevant legislation, policies and policy instruments (standards, directives, guidelines) for IT security and privacy.

All services provided by CIOB EC comply with the Operational Security Standard, Government Security Policies (GSP), Management of Information Technology Security (MITS) and departmental IT Security policies.

See Security services in section 2 for more information related to this.

3. Terms of Conditions

Term and conditions outlined below are specific to this SLA only

3.1 Duration of agreement

The term of this agreement is for a period of 1 year starting April 1, 2010 to March 31 2011. CIOB EC or CEAA may unilaterally terminate this SLA by giving 90 calendar days advance written notice to other party, or within another time frame as agreed, approved and authorized by Signing Authorities. This SLA shall be amended or terminated at the date agreed between Parties. The Client will be responsible for the effort and costs for the planning and migration of services to an alternate supplier, as applicable, following termination.

Renewal / Review

Services fees and services levels under this agreement will be reviewed on an annual basis and upon Agreement renewal. Should the review result in a change to the Services fees and Levels currently in effect under this Agreement, the proposed changes will be communicated no less than 90 calendar days prior to the anniversary or renewal date to the Client Authority to secure agreement to the adjustments before entering the next period of the Agreement.

In the event that the Client elects not to renew the agreement at the revised Services fees and levels, the agreement termination will apply.

3.2 Amendments

Request by the Client to amend this Agreement are to be done through the submission of a written document to CIOB EC and subject to acceptance by CIOB EC. Amendments requested by CIOB EC are subject to the written agreement by the Client. Amendments, once approved, will extend no longer than the current term of the SLA, be documented under a separate SLA amendment and incorporate into the main body of the Agreement during the next review of the SLA under section 4.2.

3.2 Business Escalation

The CIOB EC team will address disputes involving both parties with regards to the delivery of services initially agreed with the client. In the event they are unable to resolve a problem, the path to achieve a resolution is indicated in the table below.

Resolution Stage	Client Representative	CIOB EC Representative
Stage 1	Gilles Lévesque Manager Information Services CEAA	Chantal St-Germain Director, Business Operations Environment Canada
Stage 2	Gilles Lévesque Manager Information Services CEAA	Joanne Racicot Director, NCR Division, IT Operations & Client Support Directorate Environment Canada
Stage 3	Richard Gagné Director General Corporate Services CEAA	Joanne Racicot Director, NCR Division, IT Operations & Client Support Directorate Environment Canada

Table 3: Business escalation stage

4. Financial Terms and conditions

4.1 Services fees summary

All Services fees are subject to the following terms and conditions:

- All fees are subject to review as detailed in section 4.2
- Client agrees to pay all charges associated with this SLA
- On going fees will be prorated on a monthly basis from the date the of the Client acceptance of the SLA.

Service Name	FY 2010/2011
Fundamental services (include support/basic & Desktop/Helpdesk & Security services)	439,917.00$
IT Central Fund	86,000.00$
Applications, development & maintenance services	40,882.00$
Server Support services	20,790.00$
Database hosting services	8,190.00$
Web hosting services	16,700.00$
Telecommunications (Videoconferencing services)	232,320.00$
Blackberry services	14,868.00$
Correspondence tracking - CCMMercury	684.00$

Total	**860,411.00$**

Table 4: Services fees summary

4.2 Payment

All cost for the Services will be recovered from the Client on a quarterly basis in advance through the inter-departmental mechanism and using the financial code provided by the Client

- One time fees are due upon SLA signature;
- Issues related to the billing should be reported by the Client directly to CIOB EC.

4.3 Billing Contacts

	Client	CIOB EC
Name	**X**	**X**
Title	X	X
Address	Place Bell Canada 160 Elgin Street, 22nd Floor Ottawa, Ontario K1A 0H3 Canada	351 St Joseph Blvd Gatineau, Quebec K1A 0H3 Canada
Phone #	x	x
Fax #	x	x
E-mail	x	x

4.3 Client Financial code

IS Reference	**x**
IS Organization	**x**
Departmental Number	**x**

1. Section 1

1.1 Background

The principle of shared services is applied by large organizations around the world to improve the flow and quality of internal support services. It represents a fundamental change in organizational structure, the attitudes of the individuals who provide services to corporate personnel, and the nature of supplier-user relationships in most of the organizations that adopt it.

Shared common services are oriented around clients, performance and solutions. Clients can specify the services they need, and expect that the unit

responsible for shared services will meet their requirements. The organization, for its part, continually improves the quality of its services, increases its efficiency and reduces its costs as a result of feedback from clients.

The primary advantage of the shared common services model lies in resource optimization (cost reduction and increased efficiency). In addition, it encourages a shift towards a culture of continuous improvement through performance objectives, in addition to facilitating access to expertise and encouraging innovation and development through. The model also allows for the establishment, with other internal or external entities, of partnerships that create added value for the organization. Lastly, it allows clients to concentrate on their strategic activities.

In order to produce the desired results, the introduction of shared common services must go beyond the mere physical grouping of services and be accompanied by a "best practices" initiative aimed at improving service delivery to clients and reducing costs. The work units must obey the laws of the market when they negotiate with clients, i.e., their services must be competitive. The clients must also be able to submit comments regarding their needs and the quality of the services received. Lastly, the performance of the work units providing shared services must be subject to evaluation on the basis of measurable criteria.

1.2 Purpose

The Service Level Agreement (SLA) documents the IT services that the Chief Information Officer Branch (CIOB) of Environment Canada (EC) provides to the Canadian Environmental Assessment Agency (CEAA). It describes and quantifies the types of support that CIO Branch provides to CEAA. CIOB Branch is adopting a "one department" approach in its operation and in providing consistent levels of service across the country.

This catalogue identifies each of these services, lists the service description, service characteristics and service level objectives, (i.e. target service estimates). It also identifies the clients of the service, business processes enabled by the service, customer roles and responsibilities and how to access the service.

This service catalogue is the default, or base, service level agreement between CIO Branch and CEAA community and it will help identify what service levels we (CEAA) can expect for a particular service or product. Understanding that some organizations or groups have different requirements for services or products and these requirements will need to be negotiated, defined and signed-off in a service level agreement between CIO Branch and CEAA. If you do not have a specific service level agreement, the service levels listed in the CIO Branch Core Service Catalogue will apply.

When you contact CIO Branch for service, we should expect that the service provider will attempt to meet or exceed the target times estimated for the various services levels. However, under special circumstances like major system outages, CIOB Branch may not be able to perform the service required within these target estimates. During these times, break/fix incidents take precedence over requests for new service.

Client satisfaction will be a key driver in determining appropriate services levels and standards will evolve along with technology, time and the evolving needs of our clients. This catalogue will be updated on an annual basis with input from CEAA and consultation with CIO Branch and its vendors.

2 Parties

2.1 CEAA Information Services (client)

The information Services Group is responsible for information management (IM) and information technology (IT) provisions at the Agency.

IT responsibilities

- Administer the Agency's external & internal web sites
- Support & maintain commercial software
- Develop Agency applications
- Provide IT support and maintenance
- Manage Service Level Agreement with Environment Canada
- Provide all IT procurement for Agency
- Administer IT Asset Management
- Maintain & support videoconferencing

IM responsibilities

- Manage & administer ATIP
- Oversee Records Management
- Establish & maintain Agency File Plan
- Maintain information Management function & implement ongoing improvements
- Provide information Management training, as well as general awareness

2.1.1 General Principles and Restrictions

The Client agrees to work in partnership with CIOB EC IT Operations to make the planning, management and operation of services cost-effective and efficient. The Client agrees to the following commitments:

- To keep all owned equipment in good working order;

- To keep software licenses at the currently agreed upon version;
- To develop, in partnership with IT Operations, migration plans to ensure that client systems meet department standards;
- To meet with CIOB EC IT Operations representatives at both a senior level and a working level to review services and operations and to resolve outstanding issues;
- To ensure that any program specific applications or systems are built using departmental standard software, middle-ware and hardware. Such systems must be reviewed and approved by the department before they may be deployed if they consume departmental resources;
- To give CIOB EC IT Operations official notification prior to the occurrence of significant changes to the client organization that may have an impact on Informatics service delivery;
- To encourage the use of shared disk resources to assist in handling of information and disk capacities;
- To be aware of and follow departmental policies and procedures:
    - Policy on the Use of Electronic Networks which is found at: Use of Electronic Networks Policy.;
    - IT assets management: policy Assets management policy;
- To ensure that anti-virus software is updated weekly on remote access PCs and laptops from this site:
    - IM-IT Central - Remote PC Anti Virus Update;
- Not to disable anti-virus software on office desktop, remote access PCs and laptops. Not to disable firewalls setup for home PCs connected to the Internet;
- To ensure that security functions of user's wireless devices are activated;
- Not to connect any equipment to the network without receiving approval from CIOB EC IT Operations. This is especially true for devices such wireless access points or modems that could expose the **Econet** to attack.

2.2 CIOB EC Infrastructure Operations directorate (service provider)

CIOB EC Infrastructure Operations directorate is a partially cost-recovered organization. While the salaries and associated O&M costs for the Director and some Managers of the Branch are covered through A-Base resources, the salary and staples for specific services must be paid for through funds transferred from our clients or negotiated funds for specific projects. CIOB EC IT Operations for the NCR consists of several components.

The Infrastructure Operations Directorate is responsible for providing leadership, strategic vision and management direction for the certification, implementation and physical security of Environment Canada's IM and IT assets. These include a wide range of tools and services (Service Desk, Telecommunications, Video Conferencing, Adaptive Computer Technology, etc.) to support the operation, accessibility and availability nation wide of the department's substantive IM and IT assets.

The Infrastructure Operations Directorate also provides a wide range of security services, including the development and implementation of a national security policy, threat and risk assessments and network security tools, standards and guidelines to ensure the security of our operating environments and the integrity of the data contained within them.

The Infrastructure Operations Directorate is made up by the following five divisions:

1. Telecommunications Division
2. Data Centre Operations Division
3. Service Desk and Distributed Computing Division
4. MSC Regional Operations Division
5. IM and IT Security Division

This Service Level Agreement (SLA) also covers other services delivered by the IM and IT security division which are outlined in the various appendices of the document.

2.2.1 General Principles and Restrictions

The following general principles and restrictions are assumed to apply to all points of the SLA.

- All costs reflect the actual resources required in providing the stated service or the best estimate of those costs where history does not provide an actual cost.

- All services described reflect departmental standards and "best practices" of the information technology profession.

- All services are subject to restrictions imposed by collective agreements, the Public Service Staff Relations Act and the Public Service Employment Act.

- Hardware and software i.e. software not included under the OT suite, purchased by the client and contributed to the general infrastructure become the sole responsibility of CIOB EC IT Operations.

- Hardware and software purchased for the desktop and residing on the desktop will remain the property of the client.

- All software licensing agreements will be respected. CIOB EC IT Operations will neither support nor install unlicensed software. Client organizations are responsible for maintaining purchase/license information that can demonstrate that the software is legally licensed, in the event of an audit.

- Every effort must be made to procure client desktop and laptop hardware from the PWGSC NMSO list in order for support to be provided at the costs documented through this Service Level Agreement. Client desktop and laptop hardware purchased outside the PWGSC NMSO may be supported at an additional cost. The NCR PC Policy is found at: CIOB Branch PC Policy

- Non-departmental owned hardware will not be supported through this Service Level Agreement (e.g. employee-owned home PC's for remote access

3. Service commitment

Services are generally amortized over the life of the agreement and *pro rata* of the expected number of supported seats. As staff development is seen as a direct benefit to the user community, efforts are taken to ensure that support specialists are kept current with technologies so that they can provide support to their assigned users at the desktop. As a result staff development forms an integral part of all Services under this SLA.

The following sections describe the services that are provided by CIOB EC IT Operations. Some services are mandatory by virtue of membership in the NCR network infrastructure while other services are negotiable based on the expected level of support required by the client.

3.1 Service Standards

Services are standardized only insofar as the Client may be assured of a satisfactory level of responsiveness from CIOB EC IT Operations staff. CIOB EC IT Operations adheres to a philosophy of "best practices" service provision. CIOB EC IT Operations commits to constant review and update of its internal procedures and communications in order to provide the highest possible level of service within its resources. Input from clients is encouraged.

Client satisfaction is the yardstick against which our degree of success is measured. Client satisfaction is measured through initiatives as benchmarks.

Standard procedures for ensuring the integrity and security of the client's resources will be applied. These will include virus checking, server backup and password changes to name a few.

See Appendix 1 Service request and incident management

3.2 Catalogue Services Overview

The Service Catalogue is an integral component with the goal to further develop client relationships and improve the delivery of IT services. As such, the Service Catalogue should be designed to be an informative, easy to read and understand document that includes an Individual service sections that describe; what is included in the service, the cost and the expectations for IT and the Client in achieving optimal service delivery.

This service catalogue includes many IT services. These services are categorized under 10 main headings;

1. **Fundamental services** are the core IT services that are common to all IM/IT support of CEAA and are essential to supporting the business programs of CEAA;

2. **Desktop/Helpdesk services** are those that support employees and their productivity tools at the desktop and provide access to shared services;

3. **IT Central Fund** is a dedicated fund that represents the procurement of enterprise software and drivers.

4. **Application development/maintenance services** include application development, enhancement and maintenance of the Canadian Environmental Registry (CEAR);

5. **Server support services** are the ones that involve installation, administration, management of the servers as well as licensing;

6. **Database hosting services** for circumstances where clients will have a need to host a databases on the shared SQL infrastructure without an attached Web site;

7. **Web site hosting services** is designed for clients that require a (1) basic web site presence, without database or special application requirements and for clients that require a (2) basic Web Site presence and a content management service, including turnkey web portal services and for clients requiring (3) web application connectivity to SQL Server databases;

8. **Telecommunication (videoconferencing) services** are services related to coordinate site certifications and equipment installations, deal with support issues (equipment failures, etc.);

9. **Blackberry services** for users that connect to the server for remote access to email and other services.

10. **Security services** are services that coordinate all activities ensuring the general security and ongoing integrity of the IT infrastructure, systems and data.

.

4. Section 2

4.1 Fundamental Services

Fundamental Services are the range of CIOB EC IT Operations activities to which all clients must subscribe. This class of services comprises those that are essential to the whole operation of the NCR and **must** be in place before any other service can be provided. The NCR computing Infrastructure is worth millions of dollars in terms of the purchase, installation and maintenance of equipment. It requires constant attention so that it can continue to provide affordable, high-quality service to NCR clients.

4.1.1 Description

Fundamental services include:

- An office connection to the LAN operating at 10 or 100 Mbs
- An e-mail account on an Exchange server
- Space on a network server to provide secure storage of files
- Access to networked printers
- A remote access infrastructure supporting dialup and high speed vpn connections from home. In the past, fat client technology (office suite and other applications installed and running on home PC) were used

on home PCs but this is being replaced by thin client technology where the OA suite and other standard applications are not installed on the home PC. This will provide a more affordable, supportable and secure environment.

- A remote access service for users who are traveling anywhere in the world
- Backup and offsite storage of files on servers(e-mail, file) for disaster recovery
- High speed access to the Internet with filtering for inappropriate sites invoked.

In terms of the user's (clients) the fundamental services include:

- LAN Connection
- Email
- Space on a network server
- Print services
- Remote access (VPN)
- Backup
- Content filtering

Adaptive Computer Technology – The provision of adaptive computer technology for employees with disabilities is available.

Administration - As well as routine personnel management items there are strategic planning, budgeting and accounting and co-ordination with services, regions and national Informatics entities. Such things as monitoring and negotiating service contracts, telephones, office supplies, forms and minor hardware and software are required.

Brokerage – NCR Informatics infrastructure and services depend on the active participation of IT Operations management at several forums. IT Operations will represent the interests of the clients at these forums if the clients are not represented (e.g. GTIS).

Consultation and Feedback – Regular consultation and feedback will be conducted at the working level and the management level. Forums for these activities will normally be regular meetings of client representatives

and IT Operations representatives and the NCR IM/IT Advisory Committee.

Evergreening – In order to ensure that the existing infrastructure is kept current and does not "rust-out" a 4 year life cycle for system and network components has been implemented. This is referred to as "evergreening".

NCR Infrastructure Maintenance – Frequent maintenance is required for components of the NCR network and systems infrastructure.

Network Services - The NCR network infrastructure is very large and complex. It requires constant attention to keep it functional.

4.1.2 Service level target:

See Appendix X Service request and incident management

4.1.3 Cost

The costs in this agreement assume current levels of staff and current requirements for network capacity and disk capacity on servers. Changes in planned capacity for these and other items may require additional infrastructure and increased **evergreening** costs. Costs for Fundamental Services include staff development, the cost of server and network maintenance that are necessary to assure continued operation of our infrastructure as well as evergreening of basic networking and server equipment based on a 4 year life cycle.

These issues will be reviewed in each year of the Service Level Agreement and a capacity plan will be developed. These will be reflected in a revised **Service Level Agreement before the end of each year.**

This table shows the cost breakdown and the total cost for fundamental services.

Service	Number of users or items	Cost/User or Item	Total cost
Fundamental services	215 at head office	1,218.00 $	261,870.00 $
Fundamental services	55 in regional offices	5,000.00 $	27,500.00 $
Salary: 1CS-01 + 1CS-02			140,607.00$
O&M: 2x5,000.00$			10,000.00$
		Total	439,977.00$

Table 5: Total cost break down for fundamental services

4.2 Desktop/Helpdesk Services

Desktop/Helpdesk services are those that support clients and their productivity tools at the desktop and provide access to shared services. They may be direct services – that is, services that are directly seen or used by the client, or indirect services – those that are not seen but are nonetheless necessary to enhance productivity.

This level of service includes indirect items such as staff development, operations project management, and the like. Trouble ticket tracking and escalation is built into services.

4.2.1 Description

Desktop/Helpdesk services include:

- **Helpdesk** – All users will be provided with Helpdesk services for the departmentally approved suite of products and hardware configurations through a central number (613-953-3687) or email HELPDESK [NCR].The Helpdesk is the primary point of contact between clients and the IT Operations and all services are available via the Helpdesk.

- **Desktop Support** – All users will be provided with on-site desktop support and trouble-shooting for the departmentally approved suite of products and hardware configuration when required. The remote support (via telephone) capability will be used whenever possible with the expectation that it will improve response time and service to the clients. Application support may be provided by the Helpdesk or by on-site personnel.

They are divided into tree main levels of services: hardware, desktop and account management.

- Hardware (Computers/Laptops/Peripherals):
  - Maintain Standards
  - Incidents/Repairs
  - Installations (setups)

- Desktop Software:
  - Maintain Standards
  - Incidents
  - Install, change and remove

- Account Management:

- Windows and Network accounts
- Corporate Applications accounts

4.2.1.1 Hardware services

Maintain standards:

- Evaluate new products in consultation with the New Technologies Group.
- Establish standards for new computer and peripheral acquisitions (see Appendix II).

Incidents/Repairs:

- Initial troubleshooting and diagnosis of hardware fault.
- Determine whether it is cost effective to repair non-warranty equipment.
- On-site repair of computers, where qualified to do so, or coordination and dispatch to warranty or other service provider.
- Order parts when required.
- Coordination of loaner equipment, if required (computer/laptop and monitor only).

Installations (setups):

- Set up, configure and install Core Departmental Support computers, including laptops and peripheral devices (See Appendix I) (individual systems or small numbers of installations).
- Configure computers with the Core Departmental software.
- Configure local Windows and other network accounts.
- Set-up of other licensed business applications as required.
- Map and test network printers.
- Ensure network connectivity.
- Install supported peripherals (See Appendix I).

Replacement Rollouts:

- Management and setup of computer replacement rollouts and lease returns (large volumes).
- Delivering the new computer and managing the disposal of the old computer
- Configuring and reinstalling existing peripherals.

Moves:

- Coordinate computer moves with CIOB EC IT Operation and Facilities Management resources.
- Provide clients with instructions to complete the disconnect/reconnect of their computers.
- Assist where necessary, with disconnecting the computer, printers and peripherals at the old location and reconnecting at the new location.

- Ensure network connectivity.

Asset Inventory:
- Not included.

Not included:
Support for Non-Supported hardware.
Support for hardware or software not owned (or leased) by EC.

4.2.1.2 Software services

Maintain standards:
- Evaluate new products in consultation with the New Technologies Group.
- Establish standards for new software acquisitions.

Incidents:
- Troubleshooting and diagnosis of incidents.
- Re-installation of software.
- Escalation of incident to 3rd level technical support or to the appropriate Business Unit.

Installations, changes and removals:
- Installation, upgrading and removal of Core Departmental software on Core Departmental Support office computers (See Appendix I).
- Evaluate the installation of additional software with EC enterprise applications and core supported products.
- Verify that all software installed on equipment is licensed appropriately prior to installation.
- Deployment of updates and new releases.
- Maintenance of deployed software.

Not included:
Support for Non-Supported software.
Support for software not owned (or leased) by EC.

4.2.1.3 Account management services

Activities include creating, deleting, renaming, reactivating, disabling and/or moving of specified accounts and shared drives (with appropriate management authorization).

Windows and Network Accounts and shared drives:
- Creating, deleting, renaming, reactivating, disabling and/or moving Windows and Network accounts and shared drives.

- Installing and configuring the workstation where applicable.
- Notifying the requestor when accounts and shared drive access are created and providing the UserID and password information to the authorized user.

Corporate Applications Accounts: (e.g. Electronic Leave Reporting System (ELRS), Travel Expert System (TES), MERLIN, Results Management Tool/Financial Information Tool (RMT/FIT), etc.)

- Creating, deleting, renaming, reactivating, disabling and/or moving application accounts.
- Installing and configuring the workstation where applicable.
- Notifying the requestor when accounts are created and providing the UserID and password information to the authorized user.

4.2.2 Service level target:

Service targets for Incidents and Service Requests vary as per list below for Hardware components:

- **Maintain Standards:** Quarterly review
- **Incidents/Repairs:** Priority 2 to 4 service as per Response Times and Resolution Times Table described in the *Service Desk section*.
- Warranty repairs targets are based on the manufacturer's warranty conditions
- **Installations (setups):** Priority 2 if the user does not have any equipment; Priority 3 for new employees; Priority 4 for replacement computers where user is able to work until new equipment is ready for release.
- **Replacement Rollouts:** 14 Days and according to the current greening life cycle (every 4 years). However, at times, e.g. end of the fiscal year, large volumes of equipment are purchased at the same time. IT Operations and Client Support staff will aim to meet the service target but this may not be possible – in these cases, as schedule for the installation will be negotiated with the user representative.
- **Moves:** Minimum 14 Days lead time required (scheduling will be based on staff availability)
- **Asset Inventory:** On-going service

Service targets for Incidents and Service Requests vary as per list below for software components:

- **Maintain Standards:** review quarterly
- **Incidents:** Priority 2 to 4 service as per Response Times and Resolution Times Table. (Described in the Service Desk section in Appendix X*)*
- **Installations, changes and removals:** 5 Days

Service targets for Incidents and Service Requests vary as per list below for account management components:

- **Windows and Network Accounts and shared drives:** Priority 3 service as per Response Times and Resolution Times Table. (Described in the Service Desk section in Appendix 1*).*
- **Corporate Applications Accounts:** Requests are submitted by the Service Desk to the appropriate corporate support group for processing. Responses are provided by the support group directly to the requestor and are not subject to CIOB Service Level targets.

4.2.3 Cost

Costs for Desktop/Helpdesk services include coordinating all activities related to desktop support, hardware and software management. IT Desktop Support includes 1st level support via the Service Desk; 2nd level technical and desk side support; and 3rd level escalation when required. **This ongoing service cost is include in the Fundamental Services**.

Clients who meet one of the following criteria require support at (minimum) Level 2:

- Uses a wireless device (e.g. Blackberry, Palm Pilot etc.) connected to the server for remote access to email and other services.
- Uses Remote Access services (RAS);

Level 3 services may be requested by any client who requires a faster response.

4.3 IT Central Fund

The IT Central Fund is a centralized fund that represents the procurement of enterprise software and drivers.

4.3.1 Description

The procurement of an IT Central Fund is for all common office technology and security software such as MS Office Suite, Anti-virus, encryption, etc....

4.3.2 Service level target

None

4.3.3 Cost

This table shows the cost for the IT Central Fund per numbers of users.

Service	Number of user	Cost per user/item	Total cost
IT Central Fund	215	400.00$	86,000.00$

Table 6: Total cost for IT Central Fund

4.4 Application, development and maintenance services

This service includes application development, enhancement and maintenance of the Canadian Environmental Registry (CEAR).

4.4.1 Description

- Ensure for data integrity of the CEAR database;
- Ensure proper backups policies and procedures of the CEAR database.

4.4.2 Service level target

None

4.4.3 Cost

This table shows the cost for the Application, Development & maintenance services.

Service	Cost
Application/Dev/Maintenance – Salary: .5 x CS-02	38,382.00$
O&M: .5 x 5,000.00$	2,500.00$
Total	40,882.00$

Table 7: Total cost for Application, Development & maintenance services

4.5 Server Hosting Support Services

Server hosting support services are those that support client's physical structure that connects computers and allows them to communicate internally with servers, printers and other devices, as well as externally to the internet and this service coordinate all activities related to centralized enterprise server.

4.5.1 Description

Management of server hosting support services include:

- Installing new servers
- Installing and maintaining racks, hardware and firmware associated with the servers.
- Performing server operating system maintenance / upgrades.

- Designing and maintaining directory services (Microsoft Active Directory).
- Installing and maintaining server management software.
- Monitoring server performance.
- Troubleshooting server problems and failures.
- Planning for future capacity requirements and upgrades.
- Server backups.
- Server security.
- Researching hardware and technological developments for servers.
- Disaster planning and recovery for Departmental servers.
- Consulting and assistance with purchases of new servers.

Scheduled Maintenance Window:

Scheduled Maintenance is performed where possible outside the normal working hours. Notices regarding downtimes will be sent to clients via Exchange mail at least 3 days prior to the scheduled downtime.

Level 1 Service – Full Server Support

CIO Branch is responsible for full support of the server including: connectivity to the EC network, installation, licensing, patches and upgrades of the operating system and all applications, server performance monitoring and regularly scheduled backups.

Level 2 Service – Partial Server Support

CIO Branch is responsible for partial support of the server including: connectivity to the EC network, installation, licensing, patches and upgrades of the operating system, server performance monitoring and regularly scheduled backups. The client organization is responsible for licensing, installation, patches and upgrades of all applications on the server.

Level 3 Service – Limited Server Support

CIO Branch is only responsible for connectivity of the server to the EC network. Server will only be monitored for network loading. The client organization is responsible for the licensing, installation, patches and upgrades of the operating system and all applications. Backups and restores are the responsibility of the organization to schedule and perform. Enterprise backup facilities may be used in consultation with CIOB staff.

4.5.2 CEAA servers list

Server Name	Applications	OS (Windows)	Active until
CEAASRV01	AccessPro	2003	No end date
VMCEAAGISDEV	GIS	2003 SP2	No end date
VMCEAAGISPROD	GIS	2003 SP2	No end date
VMNCRRDIMSTS	RDIMS Dev	2003 SP2	Prévision : 30 juin 2009
ECNCRRDIMS	RDIMS Multitrans (to be transferred on CEAASRV01) Atip wwwroot (David, Francis)	2000 SP4	Prévision : 30 juin 2009
NCRRDIMS	RDIMS	2000 SP4	Prévision : 30 juin 2009
NCRRDIMSDEV	infoZone	2003 R2 SP2	No end date
NCRRDIMSINDEX	RDIMS	2000 SP4	Prévision : 30 juin 2009
SNCR01WBLL	InfoZone (Front end)	2003 R2 SP2	No end date
SNCR01ADLL	InfoZone (Back end)	2003 R2 SP2	No end date

Table 8: CEAA servers list

4.5.3 Service level target:

Service targets Server Support Service vary as per list below.

Internet availability 99% of the time
Internal network uptime 99% of the time

Level 1 Service – Full Server Support:
Hardware, network, and application(s) availability – 98%

Level 2 Service – Partial Server Support:
Hardware and network availability - 98%

Level 3 Service – Limited Server Support:
Network availability - 98% (subject to functional hardware and O/S)

4.5.4 Cost

Costs for Server Support Service services are listed below, this ongoing service costs should be renegotiated annually.

Service	Number of users or items	Cost/User or Item	Total cost
Server Support	**3**	**6,930$**	**20,790$**

Table 9: Total cost for Server Support service

4.6 Database storage hosting services

Database hosting service coordinates all activities related to data storage support.

4.6.1 Description

Management of central data storage includes:

- Installing and maintaining Storage Area Network (SAN) and other Enterprise data storage;
- Planning and allocation of data in the SAN and other Enterprise data storage;
- Installing and maintaining physical connections from the servers to the SAN and other Enterprise data storage;
- Physical maintenance of the tape library;
- Installing and maintaining Enterprise backup facilities;
- Providing Enterprise backup client software for servers;
- Performing scheduled data backups for servers using Enterprise backup facilities;
- Performing emergency user file recovery for servers using Enterprise backup facilities;
- Monitoring Enterprise backup facilities server and client performance;
- Monitoring the SAN and associated fibre switches for traffic, events and failures;
- Troubleshooting problems and failures;
- Planning for future capacity requirements and upgrades;
- Disaster recovery planning;

4.6.2 CEAA Databases list:

Database Name hosted on EC server	Data server type
NCRSQLDEVAPPS\ins1	SQL SERVER
NCRSQLCLAPPS	SQL SERVER
NATSQLCL	SQL SERVER

Table 10: CEAA databases

Scheduled Maintenance Window:
Scheduled Maintenance is performed where possible outside the normal working hours. Notices regarding downtimes will be sent to clients via Exchange mail at least 3 days prior to the scheduled downtime.

Data backup frequency (subject to scheduling changes):
Incremental: Daily
Full backup: Once a Week (kept offsite)

4.6.3 Service level target

Data Backups:
Files (users files, Shared directories): 3 months
E-mail messages: 3 months
Databases: 1 month
File Recovery Turnaround:

- Low – medium complexity 1 working days
- High complexity 3 working days

4.6.4. Cost

There will be circumstances where clients will have a need to host a database on the shared SQL infrastructure without an attached Web site. The fees for the hosting of such Databases will be as follows:

Options:

1) Non-Transactional connections from a single application

- The database is maintained by a database owner who is responsible for all modifications to the database.
- The database is used mostly for reporting and/or for lookup services

Cost: $550 per application / per annum

2) Transactional connections from a single application

- Clients can directly update the database through the application.

Cost: $2600 per connection / per annum

3) Non-Transactional connections from multiple applications

- The database is maintained by a database owner
- The database is **not** updateable by clients

Cost: $325 per connection / per annum

4) Transactional connections from multiple applications

- Clients can directly update the database through the multiple production application(s)

Cost: $2000 per connection / per annum

This table shows the total cost of database hosting service.

Service	Number of users or items	Cost/User or Item	Total cost
Database hosting	**3**	**2,730.00$**	**8,190.00$**

Table 11: Total cost of database hosting service

4.7 Web site hosting services

This service is designed for clients that require an internal or external Web Site presence, with and without database or special application requirements.

4.7.1 Description

A) Basic Web Hosting

This service is designed for clients that require a basic Web Site presence, without database or special application requirements. Clients may choose to have their own web developers manage their site. This is the minimum subscription for all clients using our services.

Cost:

- **$1600 per year**

Includes:

- 100MB of file disk space. This represents the total of the development (pre-prod) and production file environments.
- Online web site status reports
- Online statistical and link verification reports (on demand)
- Technical and client support

For clients developing their own web sites:

- Full development (pre-prod), staging and production environments
- Access to a personal shared drive in pre-production
- Access to an Online Publishing tool
- Online archiving and file restoration services

B) Content management, hosting and portal services - Web Solutions

This service is designed for clients that require a basic Web Site presence and a content management service, including turnkey web portal services. This service can also be used in combination with web applications where developers can concentrate on building their application and connect it to Web Solutions.

This service makes it dramatically easier and significantly less expensive for organizations to create and update their own web sites while fully meeting all Common Look and Feel (CLF) Guidelines and Environment Canada Web policies.

Cost:

- **Internal** Content Management with Web Solutions portal services: **$1600 per annum**
- **External** Content management with Web Solutions portal services:: **$5000 per annum**

Features:

- Content owner (any employee) can add, modify or remove information from their web site with little training and without knowing html or other programming tools;
- Role base editing;
- Very fast web site creation, reduced overall time and effort;
- Provides a tool to consistently meet departmental, Treasury Board Secretariat (TBS) Common Look & Feel (CLF), accessibility, Official Languages policies and standards;
- Based on international standards and IM-IT industry best practices;
    - All information stored in Extensible Mark-up Language (XML):
- As new policies, guidelines or best practices come out, allows for quick adoption (i.e. changes are make to the back end and then reflected on ALL sites automatically).
- Simplified maintenance including online archive access;
- Content management system and;
- Built on a commercially available content management product.

Includes:

- Site Generator – for very fast Shell Web Site creation services
- Classroom training (Web Coordinator and Content editor courses)
- Full development (pre-prod), staging and production environments
- Remote Content Management services
- Customizable Portal services
- Online archiving and file restoration services
- Others (see table 1 for more details)

C) Web Applications using SQL Server

This service is designed for clients requiring web application connectivity to SQL Server databases. Clients must already be signed up for either (also see section M) for non-web applications):

(A) Basic Web Hosting or
(B) Web Solutions content management, hosting and portal services.

Options:

1) Non-Transactional connections from a single Web Site
- The database is maintained internally by an administrator
- The database is **not** updateable by the public or external clients

Cost: $550 per connection / per annum

2) Transactional connections from a single Web Site
- The public and/or external clients can directly update the database through the production web site.

Cost: $2600 per connection / per annum

3) Non-Transactional connections from multiple Web Sites
- The database is maintained internally by an administrator
- The database is **not** updateable by the public or external clients

Cost: $325 per connection / per annum

4) Transactional connections from multiple Web Sites
- The public and/or external clients can directly update the database through the production web site.

Cost: $2000 per connection / per annum

Notes:

1. Services and charges are the same for MS Access databases. Selected Web Application technologies must meet EC standards for applications and IM-IT Architecture.
2. The *Web Application form* must be filled and submitted to the Web Services Division for evaluation as soon as possible.
3. Every web application will be required to go through our Quality Assurance Program prior to being released in pre-production or production.
4. Includes the same services listed in Basic Web Hosting or Web Solutions content management, hosting and portal services. (Refer to table 1 for complete details)

5. Includes an additional 100 MB of database data store disk space (total of development and production database environments)
6. Includes Database System Administration and other technical services required for special infrastructure/client needs.

D) Web Site Indexes and Search

This service is designed for clients requiring their own Search engine, Web Site indexes and a search interface. It is specifically designed to allow web site owners the ability to offer professional search capabilities to their clients.

This service is also available as a web services that can be called from any Operating system and development framework. It offers multi tier search service that can be seamlessly be integrated into client's web sites.

Based on *Blue Angels Technology* Metastar framework, clients may now tie into search services or utilize Web Solutions turnkey services to quickly enable search services for your web site.

Costs:

- **External** & **Internal** Environment Canada clients: **$ 600 per annum**
- **External** & **Internal** Environment Canada partnership clients and others: **$ 1000 per annum**
- **Callable Web Services** Environment Canada partnership clients and others: **$ 1000 per annum**

Includes:

- Data harvesting and indexing (maximum index collection 100MB)
- Monthly harvesting services (web site crawling services)
- Monthly indexing services (web site index building services)
- Turnkey search interfaces and results services (Based on Web Solutions framework)

Notes:

1. These charges are handled as separate items.
2. Our current search services are also known as "Web Services" that is based on the "Web Solutions core engine" in a multi-tier environment.
3. Developers can create their own calls to the search "Web Service", or client can use the Web Solutions turnkey version.
4. The current service can be called independently of the Web Server operating system and /or web development platform. (e.g.: the service can be called from a UNIX based server using python)
5. At your option, you can have your own developer build the search interface and results handler.

E) Metadata repository

This service is designed for clients requiring metadata repository services, Web Site indexes and a search interface. It is specifically designed to allow web site owners the ability to offer professional search capabilities to their clients.

Notes:

-

Costs

- TBD $$$

F) Web Mapping, GIS or Map-Based applications

For clients requiring Web Mapping/GIS services.

Notes:

- Cost is pro-rated on the current number of clients. The more clients that adhere to the infrastructure will reduce the base charges.
- Base charges can not be any lower than $4200.00
- Web mapping application can be very resources intensive. The current Web Mapping infrastructure is built on 1 server which can support an unknown number of Web Mapping Applications. This mean that we might have to purchase a new server as required and in affect change the base charges.
- Includes:
    - Web mapping pre-production and production hosting environments
    - Web Publishing tools and services.
    - On demand monthly statistical reports
    - Possibility to share shape files

Costs

- Base: For every Web Mapping Application $14500.00
- Includes:
    - Up to 1Gb (500 MB development and 500 MB production)
- SQL Connectivity $550 for each link
- Surcharge:
    - $300 / year for every extra 1Gb of file space
    - $1800 / year for every extra 1Gb of SQL space

H) Secure Server Certificate

This service is designed for clients requiring secure information exchanges between their web site and the visitor's browser.

SSL certification combines security components built into the web server and the visitor's browser to create a secured communication channel where any data is encrypted before being exchanged. Together with the help of a Trusted Certificate Authority to certify the identity of the website owner, visitors can safely enter sensitive data on a website form and be assured that the data will be sent to the correct party.

Costs:

- No charges unless you require a new certificate
- **Option A - Dedicated Certificate**
    - If you require a secure site based on your DNS address then you will have to purchase a new certificate
    - New certificate purchase 2 year web Certificate from Entrust $400

- **Option B - Shared Certificate**
    - Environment Canada clients using existing Green Lane certificate, we can add your virtual directory to use SSL to be a secured directory.

Notes:

- Even if your site uses SSL you cannot exchange information that is rated higher than Protected A
- Exchanged information must also be in line with Privacy and sensitivity policies
- We currently use Entrust Certificates

l) Domain Name Registration

This service is designed for clients requiring the reservation of their own DNS address. We offer the following services in collaboration with CMC at no extra charges:

- Reservation and form submission to proper authorities
- Coordination with CMC to estate DNS with proper IP addresses
- Email registrations in support of new DNS

Notes:

- CMC currently does not charge for their services but this might change in the future.
- Depending on your DNS request you must plan 3-4 weeks for the registration

J) Surcharges

Surcharges may be applied to Basic Web Hosting, Web Solutions, Advanced Web, Database, Search and Metadata including Web Mapping Services options. They are applied in the following manner:

- Surcharges that can be estimated will be included in the SLA at the beginning the year.
- Budget transfer requests for surcharges will also be sent in October and February to clients that have surpassed their estimated use. Online monthly reports will be available to clients so they can manage and estimate what their surcharges will be each month.
- If the charge in the SLA is too high it will be resolved with the July billing.
- The February billing will also estimate and charge until the end of March.
- If there are additional charges beyond the January estimate they will be charged in March.
- Over charges or credits will be calculated into the next SLA.

File system disk space

- Additional Data Store increment
- **30$ per annum**
- Total of development and production file space

Database Data Source disk space

- Additional Data Store increment
- **$200 per annum**
- Total of development and production file space

4.7.2 CEAA web sites list

This table list CEAA web sites.

Site Name	Web site Type
1. http://www.ceaa-acee.gc.ca/GuideQuebec	SW
2. http://atrium.ceaa-acee.gc.ca	TA
3. http://www.ceaa.gc.ca/ceartraining	TA

4. http://www.ceaa.gc.ca/ceaacentral/iam	TA
5. http://www.ceaa.gc.ca/ceaacentral/pr-rp	TA
5. http://www.ceaa.gc.ca/ceaacentral/um	TA
6. http://ecncrrdims.ncr.int.ec.gc.ca/workplan/wp_welcome_e.asp	TA
7. http://www.ceaa.gc.ca/cear	TA
8. http://www.ceaa-acee.gc.ca	SW
9. http://www.vmceaagisdev/ceaa_viewer/default.aspx	TA
10. http://www.vmceaagisprod/ceaa_viewer/default.aspx	TA
[1] (Total File Used - 100 MB) X $30.00 for each additional 100 MB.	
[2] (Total Database Used - 100 MB) X $15.00 X 12 month for each additional 100 MB.	
[3] (Total Bandwidth Used - 1 Gb) X $0.000 X 12 month for each additional 1 MB.	
SW = Static Website	
NTA = Non-Transactional Application	
TA = Transactional Application	

Table 12: CEAA web sites breakdown

4.7.3 Service level target:

Internet web site availability 99% of the time
Internal network uptime 99% of the time

4.7.4 Cost

The total cost for this service included the entire requirement to host web sites, web applications, content management or other web related services (i.e. Metastar, Index & Search, content management, Web mapping, short-term demonstration sites[12] ...).

This table shows the total cost of web site hosting service.

Service	**Total cost**
Web site hosting services	**16,700.00$**

Table 13: Total cost of web site hosting service

[12] A demonstration (demo) web site or application refers to a product that is not intended to be permanently hosted on our servers, but needs to be available for a period not exceeding six weeks.

4.8 Telecommunications (videoconferencing) services

To plan, organize, manage and deliver videoconferencing services for CEAA.

4.8.1 Description

- Coordinate technical aspects of Videoconferencing activities
- Update directory, plan upgrades, Coordinate site certifications and installations, deal with support issues (equipment failures, etc.).

4.8.2 Service level target

Videoconferencing services available to CEAA staff in strategic locations across the Department.

4.8.3 Cost

This table shows the total cost of videoconferencing service.

Videoconferencing services	**Description**	**Total Cost**
Management /Administration (salary)	-1 day per site per year CS-04 -5 days day per site per year AS-01 -1 pager call per site per year CS-02 & CS-03	$15,874.00$
Telecom links (router, name, address, SIP & CTR)		
Vancouver CEAA	gwan2, West Hastings, 10mb, 3mb	18,768.00$
Vancouver	gwvan3, Alberni, 10mb, 3mb	1,991.00$
Vancouver	gwvan3, Alberni, ISDN	7,200.00$
Edmonton	gwedm4, Airport Road, 10mb, 3mb	18,975.00$
Edmonton	gwedm4, Airport Road, ISDN	7,200.00$
Winnipeg	gwwin2, Lombard Ave, 10mb, 2mb	18,768.00$
Winnipeg	gwwin2, Lombard Ave, ISDN	18,768.00$
Toronto	gwtor1, St-Clair, 10mb, 3mb	18,768.00$
Toronto	gwtor1, St-Clair, ISDN	7,200.00$
Ottawa	gwott2, Elgin Street, 100mb, 10mb	36,087.00$
Ottawa	gwott2, Elgin Street, ISDN	21,600.00$
Quebec	gwsf1, de l'Eglise, 10mb, 10mb	7,721.00$
Quebec	gwsf1, de l'Eglise, 10mb, ISDN	7,200.00$
Halifax	gwhal1, Hollis Street, 10mb, 2mb	7,721.00$
Halifax	gwhal1, Hollis Street, ISDN	7,721.00$

Others		
Access to other ECONET sites		1,200.00$
Backups and Life Cycle management	8 routers * 4000$ * 20%	6,400.00$
Internet & SCNet		4,200.00$
	Total	232,320.00$

Table 14: Total cost of videoconferencing service

4.9 Blackberry services

PDA & Blackberry services are those that support clients activities related to maintaining the Messaging technological infrastructure for:

- E-Mail / Calendaring
- Blackberry Syncing

4.9.1 Description

Management of Blackberry includes

- Monitor and maintain the integrity of MS Exchange software on all related servers;
- Monitor and maintain the integrity of all email/calendar/public folders; databases and data components;
- 2nd and 3rd level support for Outlook / MS Exchange desktop issues;
- Analyze user requirements and recommend solutions;
- Investigate and recommend new technologies to address ongoing; client requirements;
- Support and maintenance of the servers and appropriate server and desktop licenses;
- Support of client software components;
- Evaluation, development, maintenance and upgrades of synchronization application software on servers and desktops;
- 2nd and 3rd level support for synchronization application software issues;
- Evaluation of new devices' MS Exchange compatibility to make recommendations for addition to the supported devices list.

4.9.2 List of Blackberry users at CEAA

CEAA's regions	Numbers of blackberry loaners
NCR	48
Halifax	2
Quebec	1
Toronto	1

Winnipeg	1
Edmonton	3
Vancouver	7
Total	**63**

Table 15: CEAA blackberry users

4.9.2 Service level target

MS Exchange Servers (which includes Email / Calendaring):

- 99% availability not including the scheduled maintenance window

Blackberry Enterprise Servers (BES):

- 99% availability not including the scheduled maintenance window

4.9.3 Cost

This table shows the total cost Blackberry service

Service	Number of users or items	Cost/User or Item	Total cost
Blackberry	**63**	**236.00$**	**14,868.00$**

Table 16: Total cost of Blackberry service

4.10 Security services

Security services are those that coordinate all activities ensuring the general security and ongoing integrity of the IT infrastructure, systems and data.

4.10.1 Description

Activities if this service includes:

- Enterprise IT Security
- Desktop Security
- Remote access Services

For Enterprise IT Security:

- Developing and enforcing IT security related policies that encourage best security practices;
- Developing, implementing and administering IT security training and awareness (especially for system administrators);
- Providing direction, guidance, and education to members of CIO;

- Branch and the user community to assure compliance with IT security standards and appropriate use policies;
- Creating and implementing procedures for responding to IT security incidents;
- Serving as the Departmental authority and central point of contact for IT security incidents;
- Evaluating security aspects of new technologies and define IT security requirements for implementation at EC;
- Providing consultation and risk analysis for new and existing systems, including cost, vulnerability and solutions;
- Identifying and evaluating current IT security trends and threats, and apply solutions for EC as appropriate;
- Developing and maintaining documentation and guidelines for securing the types of servers and workstations at EC;
- Investigating and participating in solutions for IT security incidents at EC;
- Investigating, implementing, and monitoring IT security tools for the Department (including firewalls and intrusion detection systems);
- Monitoring IT security and audit logs on a regular basis and resolve risks as required;
- Conducting reviews on a regular basis of IT security risks at EC and implement or recommend changes as appropriate;
- Providing technical expertise in computer and network security;
- Investigations of breach of IT Security Policies (Wireless, Acceptable Use, etc.);

For Desktop Security:

- Developing and implementing computer security software standards for desktops and laptops computers, including deployment of CEAA core applications;
- Testing, implementation, and deployment of desktop operating system upgrades and patches to desktops and laptops computers;
- Ensuring that all desktops and laptops computers centrally authenticate prior to accessing any CEAA computing service;
- Ensuring that all desktops and laptops computers are logging local security information to a central device;
- Ensuring that the Department is current in virus detection software at the office and home desktops and laptops computers;
- Monitoring the Virus Management Server;
- Updating, testing, and deploying of Virus Management Server software;
- Updating, testing, and deploying of Desktop Security Patch Management software;
- Setting up physical hardware security;
- Access to appropriate CEAA resources – i.e. Printing, network folders and files, Internet, email (i.e.: permissions);

For Remote access Services:

- All the Desktop Security activities above
- Update, configure and monitor Remote Access Servers and
- Communication Links
- Update, test and deploy Remote Access Client Software
- Implement and enforce enhanced security measures for remote
- connections

4.10.2 Service level target

For Enterprise IT Security:

- Policy violation and security incidents will be investigated on a priority basis dependant on severity and threat level to CEAA.

For Desktop Security:

- Anti-Virus updates via centralized management system. Updates can be done via push or pull technology. Minimize client downtime and safeguarding data due to viruses;
- Spyware – currently on a reactive basis via manual scanning. These rogue applications can send Departmental data to unauthorized locations, and use up bandwidth;
- Authentication prior to any connection being established outside of EC to provide accountability;
- Promote computer security by providing security awareness sessions
- To keep machines patched to current levels;
- Desktop software and configuration is done using images. Various settings are set on master images and deployed uniformly.

For Remote access Services:

- Remote Access Policy violation and security incidents will be investigated on a priority basis dependant on severity and threat level to CEAA.

4.10.3 Cost

The cost for this service is embedded in the cost of fundamental, Desktop/Helpdesk, Web, Data and Server hosting services.

Appendix 1 - Service request and incident management

Service description

Single point of contact to facilitate the restoration of normal operational service with minimal business impact on the Customer within agreed service levels and business priorities. Incident management includes initial assessment and attempt at first call resolution; prioritization and escalation and service requests.

Activities include:

- Receive telephone calls and e-mails on incidents;
- Record, classify and prioritize Incidents;
- Maintain client information (EX: location, telephone number, asset inventory);
- Provide an initial assessment and attempt first call resolution, if appropriate;
- Escalate Incident to other second/third level support IT service providers when required;
- Update the client and IT group on progress;
- Facilitate communication to clients regarding CIOB activities (e.g. maintenance or outage notifications);
- Report to Management and clients on Incident Management and Service Desk performance.

Service is available to all CEAA Staff as follows:

Core Departmental Support

For the products listed in this section, CIO Branch is committed to providing advanced support:

EX: pc configuration, usage, and troubleshooting, maintenance and repair.
Core Departmental Support products have the following characteristics:

- Products are essential to the CEAA mission
- Products are widely used across the main CEAA offices
- Sufficient support resources exist
- Valid licenses exist
- Standard

Limited Support

CIO Branch will provide minimum support for the products listed in this section. This support will be scheduled as time permits and will not take precedence over Core Departmental Support initiatives.

Limited Support products have the following characteristics:

- The use of these products must serve the interests of CEAA

- CIO Branch must be involved in the installation, but will not provide support for usage of these products
- Support must be cost-effective
- Valid licenses exist
- Hardware support is subject to parts availability and approval of cost recovery from the organization requesting the service
- CIO Branch cannot guarantee that these products or systems will work in the CEAA environment

No Support

These products have either never been supported or have been retired from the CIO Branch Support lists.

No Support products have the following characteristics:

- Products may be out of date
- The vendor may have discontinued support
- Parts are no longer available
- The product does not run in our environment or conflicts with Core
- Departmental software or hardware
- The software does not have valid licensing

Incident reports are handled on a priority basis. Calls logged to the Service Desk during core hours of operation will be assigned one of the priorities described below and action will be taken accordingly. All calls received during non-core hours will be assigned a Medium (Priority 3) priority.

Service Priority for Incident Reports

	Description	Example
Priority 1 (Critical)	An incident that denies access to services to most or all of the client community.	• Network outage on several floors or an entire building. • Primary server outage that prevents access to users' services.
Priority 2 (Serious)	An incident that denies access to services to a small group of users or to a single user.	• A portion of the network is down or a network device needs to be reset. • A users' desktop system has a hardware or software failure. • An account is not accessible.
Priority 3 (Medium)	An incident that may affect a	• Software problem

	small group or a single user. The incident does not prevent work but does impede it.	preventing viewing or printing a document • Problem accessing the Internet • Problem reading data from a group share • A service request for a new user account
Priority 4 (Low)	An incident that is annoying but does not impede the user's ability to function. Most requests for enhancements to the desktop or to individual services fall into this class.	• New software or hardware to be installed. • Remote access request • Additional network drop • Installation of a printer or other peripheral • Installation of a new PC • Installation of a new wireless device

The table below describes Response Times and Resolution Times based on the Priority assigned to an incident ticket. Other arrangements for incident resolution fulfillment may be negotiated with the user where circumstances warrant it. In all cases the user must be consulted and satisfied with the outcome.

Response Times is defined as a reaction to an incident report or a service request whereby a support specialist acknowledges the ticket, reports to the user via the automatic ticketing system, analyses the need and begins or plans corrective action.

Resolution Times is the cessation of activity related to a ticket whereby the incident has been fixed to the user's satisfaction or the user agrees that the incident cannot or should not be resolved.

Response and Resolution Times for Incidents Reports

	Core Departmental Support	**Limited Support**
Priority 1 (Critical): **Response Time** **Resolution Time**	 1 Hour 1 Hour	 N/A
Priority 2 (Serious): **Response Time** **Resolution Time**	 1 Hour 2 Hours	 4 Hours 4 Days
Priority 3 (Medium): **Response Time**	 2.5 Hours	 2 Days

Resolution Time	2 Days	4 Days
Priority 4 (Low): **Response Time** **Resolution Time**	 1 Day 6 Days	 2 Days 8 Days

It should be noted that the priority and responses above describe the maximum response time that clients may expect when reporting incidents to the Service Desk. In all cases IT Operations and Client Support staff will aim to exceed required resolution times.

Customer role

Contact the Service Desk through the access methods listed in the "How to access this service" section below.

Please have the following information available (as appropriate):

- Your name and contact information (phone, office location, Directorate or e-mail)
- Location of the affected equipment
- The CEAA computer identification number. (DOE asset tag or serial number).

Client Escalation:

Any support issues must be escalated to the Manager, Client Support for discussion with the client.

How to access this service

All clients may access this service via the Service Desk through the following methods:

Service Desk
Phone #: (819) 953-3687
E-mail: Helpdesk@ec.gc.ca

Cost

The cost for this service is embedded in the cost of fundamental, Desktop/Helpdesk, Web, Data and Server services.

Appendix 2 - IT Inventory

Inventory as of February 2010

IT Assets

Assets Type	Assets #
Physical & Virtual Servers (managed in coordination with EC in SLA)	10
Desktop	289
Laptop	170
Blackberry	62
Pocket PC	1
Printer	49
Projector	7
Palm pilot	11
Cell phone	19

IT Software

Provided or available (in coordination with EC trough the Service Level Agreement) for 215 users at Head Office & 55 users in Regional Office
Software
Adobe Acrobat Reader
McAfee Virus Scan Enterprise
Microsoft Office
Microsoft Word
Microsoft Excel
Microsoft PowerPoint
Microsoft Access
Microsoft Outlook
Microsoft Internet Explorer
Microsoft Windows XP SP2
Microsoft PeopleSoft
Sun Java Virtual Machine
Flash
Shockwave
Real Player
QuickTime
Quick View Plus
WinZip
Jetform Formflow Filler
Oracle Discoverer
CCM Mercury
Merlin

TES – Travel Expert System	
SMS – Salary Management System	
Contivity VPN Client	
I-PASS Connect	
Symantec Sygate Enterprise Firewall Solution	
Remedy, Action Request System	
Ahead Nero Express	
Apple Quicktime Player	
Canon Scangear	
Cognos PowerPlay	
CS ChemOffice Ultra	
Cyberlink PowerDVD	
Hotsync	
MultiTrans Pro – Translation	
JusAccess (web-based gateway to Legal Dept. applications)	
MSChem Station\HPChem Report	
Oracle Discoverer	
Palm Desktop	
WinZip	
S.A.S.	
CEAA specific (software manage by CEAA)	
Software	**# of licenses**
Adobe Acrobat Pro	55
Adobe Acrobat Photoshop	6
Adobe Acrobat CS2	1
Adobe Acrobat CS3	13
Microsoft Project	60
Microsoft Visio	75
Microsoft SQL Server Mgm	6
Microsoft Visual Source Safe Systems Development	6
Microsoft Visual Studio .NET Development	9
Xerox scan & PDF Pro	101
Human Concept OrgPlus	9
Privasoft (ATIP)	5
Open Text (LiveLink)	76
RedGate	2
Antidote	11
Google Earth	34
Mozilla Firefox	6
Opera	1
WS FTP Pro	2
Norton – Partition & Design	2
Corel Draw	1

ESRI ArcGis Server	1
ESRI ArcGis ArcView	2