Environment Canada Environnement Canada

Audit of Governance of Specialized IT Resources

May 2010

Canada

Key dates

Opening conference date (launch memo)	May 2009
Audit plan sent to management	September 2009
Closing conference date (exit debrief)	March 2010
Audit report sent to management	May 2010
Management response received	May 2010
Penultimate draft report approved by Chief Audit Executive	May 2010
Audit committee recommended	June 2010
Deputy minister approval	December 2010

Prepared by the Audit and Evaluation Team

Acknowledgements

The audit team, composed of Darine Tabbal, Graça Cabeceiras and Kenneth Gourlay under the direction of Jean Leclerc, would like to thank those individuals who contributed to this project and, particularly, employees who provided insights and comments as part of this audit.

Original signed by

_____

Chief Audit Executive

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The delivery of information management (IM) and information technology (IT) services in a scientific department like Environment Canada (EC) is a complex issue. Aside from cross-cutting services like IT security, infrastructure management, operations and the development of office applications, scientific departments must also develop and implement complex scientific systems, often involving complex data capture and manipulation in a real-time environment, the modelling of complex systems, and the in-depth analysis of model output to allow for forecasting of trends.

Over the past few years the Department has undergone some major transformations, including the creation of a Chief Information Officer (CIO) reporting to the Deputy Minister and the shift from regionally delivered services to nationally delivered services.

During these transformations, many IM and IT staff were moved out of the program areas that they had traditionally served and into a new centralized service organization under the CIO. The staff that moved to the new organization were generally meant to be those who deliver generic IM and IT services. While IM and IT staff with highly specialized skill-sets were not migrated to the Chief Information Officer Branch (CIOB), in recognition of the need to have these staff closely associated with the scientists that they support, the Deputy Minister made it clear that they were to receive functional direction from the CIO.

In its recent Directive on the Management of IT, Treasury Board (TB) has assigned the governance of IT activities to the CIO of each department.[*] Past management accountability framework assessments for the Department have identified opportunities for improvement in the area of its governance of these non-CIOB staff and the IT services that they deliver.

Throughout this report, staff carrying out IT activities in the program areas are referred to as **embedded IT staff** and the IT work that they carry out is referred to as **specialized IT activities**.

Overall objectives and scope

The objective of this audit was to provide assurance that the governance of specialized IT activities and selected, specialized IM activities in EC, and the risk management and controls supporting this governance, are adequate and sufficient.

This audit focused on specialized IT activities, in the context of the overall governance of IT activities in the Department. During the development of the audit program, this focus was expanded to include specialized IM activities related to the management of Crown data captured and maintained by the Department.

This audit was included in the departmental Audit and Evaluation Plan 2009–2010 as approved by the Deputy Minister, upon recommendation of the External Audit Advisory Committee.

Statement of assurance

This audit has been conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and the Policy on Internal Audit of the Treasury Board of Canada.

[*] Directive on the Management of IT (2009)

In our professional judgement, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on a comparison of the situations as they existed at the time, against the audit criteria.

Summary of findings and conclusions

In recent presentations[*] the CIO has assessed his organization's IT maturity[†] to be at level 1 (reactive) with pockets of activity at levels 3 (service) and 0 (chaotic). CIOB notes that recent accomplishments have put it firmly on the path toward a solid maturity rating of 2 (proactive). Their target is to attain a maturity level of 4 (value), which implies that the organization will have become a strategic business partner. This assessment aligns fairly well with the observations made in this audit that **steps are being taken in many areas to address current weaknesses in the governance of specialized IT activities**.

Our conclusion that the current overall level of governance for specialized IT activities is not yet adequate, and that a number of changes are required to allow the maturity level to rise, is a reflection of where the Department is on the maturity curve and supports continued activity to raise the overall maturity rating. These changes can be grouped by governance themes as follows:

Governance structure and process ownership

In order to ensure that IT resources are allocated to activities that are aligned most effectively to departmental priorities and objectives (including program outcomes and results), there is a need to provide more clarity surrounding the committee structures that make IT investment decisions. To accomplish this, it is first necessary to establish the ownership for each of the IT processes that are carried out in the Department. This theme has been addressed in Recommendations 1 through 3 of the report.

Delivery of service – establishing what, who and how

Establishing what work will be carried out in the program areas, who will carry out the work and how that work will be conducted also must be clarified. What work should be carried out by embedded staff is the subject of recommendation 5. Within the context of the process ownership environment established in recommendation 2, the criteria for determining which IT staff should be embedded in the program areas are the subject of recommendation 9. Establishing the standards and architecture within which specialized IT activities will be carried out is the subject of recommendations 6, 7, 8 and 10. This theme will address issues of management of change, methods of engagement, training and communication.

Monitoring and reporting

In order to ensure that governance is adequate, investments are optimally aligned with priorities, and there is adequate oversight and compliance, the CIO will have to provide mechanisms for monitoring the activity of embedded IT staff and tools for

[*] External Audit Advisory Committee meeting of January 2010
[†] Using a maturity scale developed by Gartner Inc., which can be found in Annex 4
Maturity Levels
(Source: Gartner Inc., April 2006)

reporting on those activities to all boards and the Executive Management Committee (EMC) (within the context of complete reporting on the run, renew and transformational activities)

The major risk to the Department arising from these findings is that, without a clearly defined IT governance structure to define what needs to be accomplished, a clear understanding of who will provide the work and how they will carry it out, and the capacity to monitor and report on the full range of IT activity, the Department may not have the necessary information to make good IT investment decisions or take advantage of efficiencies that can be reinvested in new and transformative initiatives. These factors may result in a diminished capacity to ensure program delivery objectives.

Accomplishing these fundamental changes will require the co-operation of all parties. In particular, as the CIOB's maturity level continues to rise and as it continues to roll out its service catalogue for IT services, program Assistant Deputy Ministers (ADMs) will have to commit to using services from the catalogue where they exist and where they are a good fit for required IT activities.

RECOMMENDATIONS

1) EC's governance structure should clarify how IT investments, both within CIOB and the program areas, align to EC strategic imperatives, program outcomes and results (program activity architecture), and how they are incorporated into EC's integrated investment planning process.

Accordingly, the CIO, in consultation with EMC colleagues, should develop and present for board and EMC discussion and approval an updated IT demand and supply governance structure. To assist with this effort, the CIO should work with the Chief Financial Officer (CFO) to ensure that financial coding for expenditure reporting is sufficiently granular to ensure appropriate accounting, monitoring and reporting of IT-related expenditures for an EC view.

Furthermore, and in support of the above, the CIO should confirm plans to provide EMC with better data on IT demand-and-supply-related expenditures, in order to make the case for, and help executives prioritize, IM and IT investment decisions. This would include periodic reporting on IT resource utilization and allocation in support of run, renew and transformational expenditures.

2) Established IT processes should result in the greatest value being created for EC (such as development or testing of applications, having criteria to decide when development should be carried out in the program area rather than CIOB, etc.).

Accordingly, the CIO, in consultation with EMC colleagues, should establish and broadly communicate an ownership framework for all IT processes (such as for the development or testing of applications).

This ownership framework should define:

- who will own each process and in what situations, and who is accountable to execute which parts of the process;
- the functional reporting relationships that will exist between the process owners and the CIO; and
- the line reporting relationships that will exist between these same process owners and the client program areas.

3) The CIO, in consultation with EMC colleagues, should ensure that adequate mechanisms exist for making IT investment decisions (including investments for ongoing operations and investment decisions for embedded IT staff and their associated activities) in the new integrated planning process. The resulting plan should be presented to EMC for ratification of cross-board priorities and for approval.

4) The CIO, in consultation with the ADMs responsible for program delivery and with the assistance of the CFO, should develop better tools for reporting the expenditures made in IT. These tools should give the boards and EMC a complete breakdown of all expenditures in IT, including those required for the maintenance of the infrastructure and operations, and they should allow branch ADMs to report on the extent and nature of all IT activity being carried out in the program areas so that the boards and EMC can review the investment decisions that have been made.

5) The CIO, in consultation with the ADMs responsible for program delivery, should create criteria for deciding when it is appropriate for program areas to carry out IT activity. Once created, the criteria should be presented to the EMC for approval.

6) Building on the strong work already being undertaken as part of the transformation of CIOB in the areas of architecture, processes and standards, the CIO should, in consultation with the ADMs responsible for program delivery, establish mechanisms to engage programs/clients in developing, broadly communicating, and publishing EC's Enterprise Architecture Vision, processes and standards. This would include program area participation as members of the Architecture Review Board.

Further, the CIO, in consultation with ADMs responsible for program delivery, should establish and implement mechanisms for appropriate oversight, monitoring and reporting of IT activity, to assure compliance with standards and optimal use and investment of IT resources.

The CIO, in consultation with ADMs responsible for program delivery, should establish an IT resource "blueprint" comprising competencies, knowledge and skills standards, and training and learning.

7) The CIO, in consultation with EMC colleagues, should establish an enterprise data management program that includes, as a minimum, a sustainable centralized inventory of Crown data under the custody of the Department. This inventory should include (but not be limited to) information about: the nature of the data that is held; the volatility of the data; the source(s) and location(s) of the data; the contact information for the appointed steward of the data; and the criticality or sensitivity of the data.

This centralized inventory (corporate metadata repository) should be the system of record for departmental metadata, and departmental processes should be established to ensure that appointed data stewards create and maintain the metadata for all data of business value. Data producers, consumers and data management systems across the Department should reference and update this corporate metadata repository when inquiring about the existence of departmental data.

8) The ADMs responsible for program delivery should ensure that all departmental databases under the control of their branch are represented in the corporate metadata repository.

9) The CIO, in consultation with ADMs responsible for program delivery, should create criteria for deciding when it is appropriate for program areas to staff IT-related positions. The criteria should:

- clearly define the scope and nature of the roles these staff will play, and define the functional relationships that these staff will have with the CIO;
- be accompanied by directives and guidance on the use of architecture, standards and procedures for conducting the IT activity.

10) The CIO should ensure that newly hired IM and IT employees receive mandatory orientation on standards, architecture and IT processes. Further, the CIO should ensure that CIOB places no impediments in the way of embedded IT staff attending any IT training that is available to CIOB staff.

11) Program ADMs responsible for specialized IM and IT personnel should:

- ensure that branches develop specific succession plans for each employee (or group of employees) who has a specialized skill set that is necessary to carry out a given job;
- ensure that employee training and development plans for embedded IM and IT staff include training on departmental architecture, standards and processes; and

- ensure that specialized IM and IT activities are carried out by properly qualified staff.

1 INTRODUCTION

This audit was included in the departmental Audit and Evaluation Plan 2009–2010 as approved by the Deputy Minister, upon recommendation of the External Audit Advisory Committee, in May 2009.

1.1 Background

The subject area for the audit was an area of high risk identified by the Chief Information Officer (CIO) during interviews while preparing the audit plan. The CIO expressed concern about our ability to speak to the governance of information management (IM) and information technology (IT) activities in the Department as a whole, because the extent and nature of the activities that are being carried out in the program areas was not transparent.

Preliminary survey work for the audit was carried out from April 2009 to July 2009. The audit program was prepared and approved in August 2009, and the audit fieldwork was carried out between September 2009 and December 2009.

The Treasury Board Secretariat's (TBS's) Organizational Readiness Office and the CIO's Council have established three "generic" models for delivering IT services within the Government of Canada, one each for large, medium and small departments and agencies. Common to all of these models is the centralized delivery of IT services with all IT staff reporting to a CIO. In this report, these generic models for IT service delivery will be referred to as CIO models.

In 2005, Environment Canada (EC) embarked upon a process to transform IT services from a highly decentralized model to a centralized model, creating a new Chief Information Officer Branch (CIOB) in the process. To deliver on this transformation agenda, the Department named a CIO and adopted a modified CIO model for large departments and agencies. The Department's Executive Management Committee (EMC) supported the creation of this organization and its mandate in 2007.

Under the old model, IT services had been delivered and governed in a very decentralized fashion. Each program and region had their own IT delivery mechanisms and governance strategy. The modified CIO model was meant to operate in a way that can be thought of as centralized delivery of standard IT services (delivered by CIOB), augmented by centrally governed but program-delivered specialized IT services. The new model was also meant to support the Department's move to a set of nationally delivered services rather than the regionally delivered services that had been in place prior to the transformation.

Although the CIO model developed by TB is based upon providing IT services centrally, in a scientific department like EC, program delivery often depends upon IT staff with highly specialized skill sets working in a real-time computing environment. These skills are often not generally available in the wider IT community. For example, the community of developers that can do algorithmic development in a real-time programming environment, such as those delivering EC's weather and climate modelling services, is very small.

The modification to the CIO model was intended to allow IT staff that had these specialized skill sets to remain in the program areas while receiving functional direction from the CIO. As a result, many of the IT staff that had been embedded in the program

areas prior to 2005 were moved to the newly created CIOB during the transformation, including most of the staff that had been delivering traditional IT activities. Many of the IT staff with specialized skill sets were left within the program areas to receive line direction and to carry out their specialized IT activities.

In this audit report, development IT activities that are carried out in the program areas and that require specialized technical or subject matter skills will be referred to as **specialized IT activities**, while staff members who deliver the services are referred to as **embedded IT staff**.

EC's 2006–2007 management accountability framework (MAF) assessment found that the CIO had direct control over only 80% of the computer systems (CS) community, raising a question about the level of governance over the remaining 20% of the community that resided in the program areas. This created an "opportunity for improvement" rating on the level of corporate engagement in IT management.

Work carried out during the preliminary survey confirmed that the 2006–2007 MAF assessment was still valid. Using information from the Human Resources Management Information System, we found that 16% of all non-vacant CS positions resided outside CIOB. To obtain a complete picture of specialized IT activity it was also necessary to consider embedded non-CS staff who carry out IT activities. Including this group, the MAF estimate of embedded IT staff appears to still be reasonable.

The most recent round of MAF assessments highlighted two other areas where there were still opportunities for improvement in the stewardship area. Business continuity planning and the management of IT security were areas of concern to TBS, because a department cannot protect resources or continue to provide services of which it is unaware.

Because specialized IT activities in the Department represent such a significant investment, the governance of those activities is critical to ensure the security of departmental resources and the continuity of the critical services that the activities deliver. As both of these areas have been the subject of a recent audit, they were only addressed peripherally during the current audit. However, given the highly specialized nature of the skills required to do this type of activity, recruitment and retention (including succession planning) becomes a very important factor for ensuring the continuity of services delivered by embedded IT staff. For this reason, succession planning was a specific factor considered during the audit.

During the preliminary survey, one of the program executives expressed concerns about whether the full extent and nature of the scientific data within the Department was known. This led to a discussion about whether staff have a common understanding that data created or captured by the Department are owned by the Crown. The imperative for scientists to "publish or perish" was also discussed, as it may lead certain scientists to assume personal ownership of the data they capture rather than recognizing that the data belong to the Crown.

To accommodate this concern, the scope of the audit was extended to include the governance of data resulting from specialized IT activity in EC. However, as there is a planned audit to address the overall governance of IM in fiscal year 2010–2011, we decided to restrict the scope of activity in this area to the governance of Crown-owned scientific data sources created or collected by the Department. We note, however, that IT activities do not function in isolation and that IM activities form part of the four domains of IT activity identified by the Office of the Comptroller General.

Another indicator that received an "opportunities for improvement" rating in the 2006 and 2007 MAF assessments was the measurement of the value derived from IT investments. TB's new Directive on Management of Information Technology reinforces the need for this requirement, by giving the CIOs the responsibility for monitoring and measuring IT management performance using both governmental and departmental key performance indicators. Discussion on this topic led us to look at how specialized IT activities are reported to the CIO so that the CIO can meet monitoring requirements set out in the Directive.

1.2 Objective and scope

The objective of this audit is to provide assurance that the governance of specialized IT activities in EC, and the risk management and controls supporting this governance, are adequate and sufficient.

This audit focused upon specialized IT activities, in the context of the overall governance of IT activities in the Department. The scope also included an IM focus that was strictly related to the management of Crown data captured and maintained by specialized IT resources or in the systems that they develop. It included an investigation of the governance of embedded IT staff, as the quality of governance that staff receive will reflect upon the governance that is provided to applications and assets.

The audit was national in scope, and included interviews with staff from the National Capital Region and a number of regional offices.

1.3 Methodology

As per the TB Internal Auditing Standards for the Government of Canada and the Institute of Internal Auditors' *International Professional Practices Framework*, assurance has been provided through the following methodologies:

- Interviews – During the preliminary survey, we conducted interviews with the CIO, two of the three program Assistant Deputy Ministers (ADMs) responsible for specialized IT activities, and each of the Directors General in CIOB (often during focus groups that included their senior staff). During the conduct phase of the audit we conducted 35 interviews of embedded IT staff or their managers (including a number of CS staff working in the IM field). During the reporting phase we carried out a Department-wide debriefing session where our findings were presented (to any embedded CS staff or manager who wished to attend), and we conducted individual debriefings of the findings and recommendations with program-area ADMs and the CIO.
- Sampling and testing – We determined which IT staff and managers to interview based upon a stratified random sample of known embedded staff, augmented by auditor judgement and information gleaned during the preliminary survey. This sample was not sufficiently large to be used for estimation of error rates, but it was believed that it would be sufficient to allow us to investigate and conclude on major areas of concern.
- Documentation and data analysis – During the audit we reviewed numerous documents received from the program areas, interviewees, websites and SharePoint/Ecollab collaborative sites.

The criteria that defined our expectations in this audit are based on the control objectives outlined in the Control Objectives for Information and related Technology (COBIT 4.1) framework for IT governance. The criteria can be found in Annex 1 below.

COBIT is an internationally accepted framework for the governance of IT, focusing on the processes that are necessary to carry out IT activities (including IM functions). In an annex to its Financial Management Policy Framework, TB has endorsed COBIT, stating:

> "Control framework(s) for information technology (IT) in relation to internal control over financial reporting…. Is a suitable control framework for information technology (IT) in relation to departmental internal controls over financial reporting and access security processes. Treasury Board recognizes that such IT frameworks should include at least:
>
> - *CobiT (Control Objectives for Information and related Technology)* for IT control objectives embedded in financial and information systems; and
> - *Government Security Policy (GSP),* including Treasury Board related IT control policies, as approved by Treasury Board."[*]

In its Government of Canada IT Services Program Framework, TB further endorses COBIT when it says:

> "COBIT provides an industry best practice reference model of common IT management and governance processes within four groups: Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. ITIL provides a framework of common IT processes for the service delivery and service support processes (IT Service Management Framework)."[†]

1.4 Statement of assurance

This audit has been conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the TB's Policy on Internal Audit.

In our professional judgement, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on a comparison of the situations as they existed at the time, against the audit criteria.

2 FINDINGS AND RECOMMENDATIONS

CRITERION 1: Roles and responsibilities are established

2.1 General comments for Criterion 1

Despite the EMC's 2007 decision to support the creation of CIOB and the Deputy Minister's support for the proposal to "proceed with their [CS employees who are still

[*] Report of the Senior Committee on the Review of the Financial Management Framework of the Government of Canada, Annex E-3 (www.tbs-sct.gc.ca/fm-gf/ktopics-dossiersc/gapr-pcrg/framework-cadre/framework-cadre12-eng.asp).
[†] Profile of GC Information Technology Services, Chapter 3.0 (www.tbs-sct.gc.ca/cio-dpi/webapps/technology/profil/profil04-eng.asp).

external to CIOB] integration and/or to establish a functional relationship with CIOB," at the outset of the audit the CIO's accountability for embedded IT staff was not entirely clear. Senior executives in the program areas questioned the CIO's authority over embedded resources, and senior staff within CIOB noted that they had never seen this authority expressed in writing. Concurrent with the conduct of the preliminary survey for this audit, TBS released the Directive on Management of Information Technology, which came into effect on April 1, 2009. This directive defines information technology as follows:

> "Information Technology involves both technology infrastructure and IT applications. Technology infrastructure includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. IT applications include all matters concerned with the design, development, installation and implementation of information systems and applications to meet business requirements."

It goes on to clearly state that the departmental CIO has responsibility for IT governance, IT planning, IT strategies, and monitoring and reporting.

2.2 The governance structure that exists for IT is not clearly defined

COBIT states that "IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives"

Although the internal organization of CIOB and the processes that are implemented to carry out IT activities are important characteristics for the governance of IT, they are not the focus of this section of the report. CIOB's organization is discussed briefly in section 2.3 below and the processes for carrying out IT activities are dealt with in sections 2.3 and 2.7 below. This section focuses on the leadership aspects of IT governance, including the governance structures that exist for IT within the Department. These include the committee structures that set overall priorities for the IT activities in order to ensure alignment of IT activity with organizational objectives and to ensure that performance measurement processes exist for the CIO to report on the effectiveness and efficiency of the IT activities.

In this context, we expected to see an official, well-documented, well-communicated committee structure for the governance of IT in the Department, one that defines unambiguous accountability and recognizes the CIO's responsibilities under the TB Directive on Management of Information Technology.

The only document we could find that described the governance structures for IT was a draft model that CIOB had created (referred to hereafter as the "supply and demand model") for an IT governance structure that is loosely based upon a supply and demand governance model articulated by Gartner Inc. We note that Gartner considers this type of model to be an industry best practice.[*] We found evidence that the model was

[*] Getting More for Less: Best Practices for Demand and Supply-side Governance, PPMIT1_104, p. 5, Michael Gerrard, Gartner Inc. (2009).

communicated widely within CIOB at “town hall” meetings, but it is not clear how extensively the model was circulated in the program areas.

The supply and demand model (reproduced in Annex 3 below), as its name suggests, segregates governance into a supply side and a demand side. The demand side of the model defines what IT services are required to carry out the Department’s objectives and to determine the relative priority of each of these requirements. The supply side of the model deals with how the required services will be provided.

The program boards and regional committees are at the apex of the demand side of the model, ensuring alignment with board priorities. The program board website states that the program boards are “responsible for direction, priority-setting, planning and reporting and recommending resource allocations for the Strategic Outcomes and related Program Activities. Boards ensure that there is horizontal coordination on policy and program issues and address key PAA Program related policy and management issues and refer them to EMC as appropriate.” We also note that the CIO sits as a member of two of the program boards, which indicates CIO awareness of priorities arising from board discussions. We find that this evidence supports the inclusion of the program boards in the governance structure for IT.

The inclusion of regional committees on the supply side of the supply and demand model is an area of contention because all programs are now nationally delivered and that implies that regions should not have any IT priorities that differ from those established by the boards. We find that this area of contention should be addressed before adoption of this or any IT governance model, in order to reduce the chance of confusion in roles and responsibilities.

We observed that, while the program managers did not always speak of governance committees in the same terms as those used by CIOB, they all identified their board as the body responsible for priority setting in their program, including IT priorities.

We observed that the supply and demand model does not explicitly include all of the committees that govern IT activity in the program areas, such as the Technology Transfer Advisory Committee (TTAC) in the Weather and Environmental Services (WES) board, but that it does not preclude activities by this type of committee. TTAC, and other committees of this nature that have defined mandates, roles and responsibilities and well-documented activities (such as providing a quality assurance role in the implementation of scientific modules), are examples of best practices for IT governance within the program areas.

We were also informed about other committees that support the boards in decisions surrounding IT governance, such as the WES board’s Directors General committee. Although we were told that this type of committee forms part of the IT governance structure, we found no evidence of a written mandate or objectives for these committees, or procedures for bringing IT needs to their attention.

The apex of the supply side of the supply and demand model resides within CIOB, which implies CIOB oversight over how IT activities are carried out in both the programs and in CIOB–which is in line with the Directive on Management of Information Technology.

We note that all of the four domains described by the CIO model for large departments[*] (**Architecture:** planning/enterprise architecture/client portfolio management; **Operations:** infrastructure/operations and security; **Development:** application

[*] TBS Community Generics website: organization chart for large IT organizations .

development / database and data administration; and **Information Management:** IM / knowledge management) are included on the supply side of the proposed supply and demand model (the CIO uses the phrase “run, renew, transform” when referring to these domains of IT activity). We note that while the program boards are represented on the supply side of the model through the portfolio management function, the model makes no explicit reference to the governance of IT activity that is provided directly by the program areas.

Finally, aside from EMC, we observed no mechanism to allow competing priorities arising from different boards for the use of finite CIOB resources to be discussed, prioritized and resolved. Although EMC is capable of performing this function, it is unlikely to have the time necessary to address this type of concern on a day-to-day basis.

Given the contention surrounding the inclusion of regional committees on the demand side of the supply and demand model, the exclusion of explicit references to the activity of embedded IT staff on the supply side of the model, and the lack of a mechanism for resolving competing IT priorities across boards, we find that the governance structures for providing leadership and direction to specialized IT resources are not adequate.

2.2.1 Impact

In the context of specialized IT activities, ambiguity around the governance structure for the delivery of IT services may lead to confusion. This confusion can make it more difficult to assure the alignment of IT activity with business priorities, reducing the value that IT provides to the organization and reducing the opportunities that may exist for identifying savings that can be reinvested elsewhere in support of program delivery. Another possible impact of confusion is that it may lead to conflicts that erode the Department’s ability to work toward a common set of goals.

2.2.2 Recommendation

1) EC’s governance structure should clarify how IT investments, both within CIOB and the program areas, align to EC strategic imperatives, program outcomes and results (program activity architecture), and how they are incorporated into EC’s integrated investment planning process.

   Accordingly, the CIO, in consultation with EMC colleagues, should develop and present for board and EMC discussion and approval an updated IT demand and supply governance structure. To assist with this effort, the CIO should work with the Chief Financial Officer (CFO) to ensure that financial coding for expenditure reporting is sufficiently granular to ensure appropriate accounting, monitoring and reporting of IT-related expenditures for an EC view.

   Furthermore, and in support of the above, the CIO should confirm plans to provide EMC with better data on IT demand-and-supply-related expenditures, in order to make the case for, and help executives prioritize, IM and IT investment decisions. This would include periodic reporting on IT resource utilization and allocation in support of run, renew and transformational expenditures*.

* Run, Renew and Transform is defined in Annex 5 Acronyms and Terms

2.3 The ownership framework for specialized IT processes is not clear

Both TB and COBIT assume that IT processes will be owned by the CIO. As a result, the requirement to establish ownership for IT processes normally means that the CIOs must assign ownership for each IM or IT process to someone in their organizations. Establishing process ownership is important because it supports the effective establishment of roles and responsibilities for IT, and provides a mechanism for assigning accountability for the quality of governance being provided.

The focus of this section is on how the Department has chosen to establish ownership over shared processes such as the development of applications, the establishment of standards and architecture, and the management of information in EC. By way of example, in the case of development, this section will focus on who owns the development processes for specialized IT activities that are carried out in the program areas, and who is therefore responsible for providing guidance, leadership and direction in that regard.

In 2007 the Deputy Minister made it clear that, with respect to embedded IT employees, the CIO needed to either "proceed with their integration and/or to establish a functional relationship with CIOB." During the audit we observed that IT staff are still embedded in the program areas and that they are still carrying out specialized IT services. As the remaining embedded IT staff have not been integrated into CIOB, we expected to find that a functional relationship would exist between them and CIOB.

As was noted earlier, we observed that for activities carried out entirely within CIOB, process ownership has been established by the Department's adoption of the modified CIO model. For the remaining activities, carried out in the program areas, we found no evidence of any formal agreements between the CIO and the program areas regarding sharing or delegation of ownership for these processes. Although we observed that while the CIO sits as a member of two of the program boards and CIOB staff are often directly involved in large-scale IT activities being carried out in the programs, we found that these relationships are not sufficient for the CIO to claim to have a functional relationship with the embedded IT staff as was required by the Deputy Minister in 2007.

When looking at roles and responsibilities, we found two distinct types of work being carried out by embedded IT staff. The first type of work includes development/testing and implementation work that requires highly specialized scientific knowledge (such as that required to maintain the numerical models supporting weather services). We note that this specialized work was often associated with large-scale projects that would garner the attention of the governance boards due to their size, transformational nature, risk profile, complexity, or alignment with current priorities.

The second type of work includes more generic IT activities such as database maintenance or the development and maintenance of web applications. We found no formal criteria to explain why embedded IT staff carrying out this type of generic IT work were left in the program areas. This issue is discussed more fully in sections 2.6 and 2.9 below.

We observed that process ownership and the associated roles for embedded IT staff tend to be better defined for large projects, with all parties having a better understanding of their boundaries (their roles and responsibilities, the roles and responsibilities of their CIOB colleagues, and the interface between their two groups), and that staff in these

larger projects often reported very good co-operation between CIOB staff and embedded IT staff.

We further observed that larger groups of embedded developers and data managers tended to have better-articulated roles and work more closely with their CIOB counterparts than single individuals or smaller groups of embedded IT staff who tended to work in isolation.

We observed that managers and staff in the regions occasionally spoke of priorities for IT activity that differ from those expressed by the boards. Demand arising from the regions tends to be for IT activities in support of existing applications and databases (activities for "keeping the lights on"), while demand from the boards tends to be more focused on new initiatives. This split in the demand side of the supply and demand governance model is reflected in the governance model, which shows the priority management boards and regional committees at the same level; but as noted in section 2.2 above, this inclusion of regional committees in the model is an area of contention with management in the program areas, as it would appear to allow for regional differences in service delivery. We note that executives in the programs have uniformly stated that all program priorities arise from the boards, and that demand arising from the regions is either a misunderstanding of board priorities by regional managers and staff or a result of these staff and managers not knowing how to bring IT demand issues to the board for prioritization.

Managers in the regions where program staff are co-located with CIOB staff occasionally reported having used "pre-transformation" relationships to have their priorities met. Managers in regions without recourse to these pre-existing relationships tended to be more frustrated, and reported more often that they do not know who to contact in CIOB to get work done. It is not clear if the nature of the work being carried out via these pre-transformation relationships is being fully reported to the CIO or being done "off the corner of the desk" (i.e., activities that are carried out with no budget or mandate but that are often critical to the success of the organization or initiative).

We observed that, in the community of embedded IT staff, the ownership of processes for acquisition of IT equipment and support of operations was fairly uniformly accepted to reside within CIOB. We observed that ownership and roles were generally better defined for the acquisitions and operations processes. Although we note that comments from the program staff were largely positive about their relations with operations, we did observe one exception to this general satisfaction: the support that has been available to the program areas for maintenance of their older IT assets since the creation of CIOB. We observed that many IT assets that had been acquired by the program areas prior to the transformation are not being adequately maintained. During the transformation, many of the CS staff that had been managing these assets were transferred to CIOB, but the responsibility for maintaining the assets seems not to have been transferred with the staff. We observed that this situation was especially true in many of the Department's laboratories. We observed that CIOB's Operations Directorate has recently begun to identify these legacy IT assets, and has begun negotiations to bring these assets under their management.

We also observed that the CIO is using a variety of methods to communicate the roles and responsibilities of CIOB staff, both to clients and within the branch. These methods include participation in projects by portfolio managers and client relationship managers (CRMs), "town hall meetings," presentations, websites, collaborative tools (such SharePoint and Ecolab sites), and email communication of important decisions and

performance metrics. We observed that weekly “routine orders” are distributed to all CS staff, including embedded CS staff, and that CSs within CIOB are required to read them. Based upon the interviews we conducted, the level of penetration that this communication is achieving within IT staff embedded within the program areas is unclear.

Managers in the program areas reported that the recent implementation of the CRM roles and portfolio management roles within CIOB has improved their understanding of the internal workings of CIOB, and these managers often praised the relationship they had with their portfolio manager or CRM.

2.3.1 Impact

Not having a clear owner for IT processes means, for example, that accountability for ensuring adequate governance and oversight of the development process is diffused throughout the organization. This may lead to poor decisions being made about IT investments, resulting in lost opportunities for reinvestment and reduced value being derived for money spent.

If roles and responsibilities are not well defined and are unambiguous, and/or if they are not well communicated, actors and stakeholders do not know who to contact to perform a given task. This may lead to confusion, delays, gaps in activity (when no one assumes responsibility for a task), or wasted resources (when the same task is duplicated or where two tasks work at cross-purposes).

2.3.2 Recommendation

2) Established IT processes should result in the greatest value being created for EC (such as development or testing of applications, having criteria to decide when development should be carried out in the program area rather than CIOB, etc.).

   Accordingly, the CIO, in consultation with EMC colleagues, should establish and broadly communicate an ownership framework for all IT processes (such as for the development or testing of applications).

   This ownership framework should define:

   - who will own each process and in what situations, and who is accountable to execute which parts of the process;
   - the functional reporting relationships that will exist between the process owners and the CIO; and
   - the line reporting relationships that will exist between these same process owners and the client program areas.

CRITERIA 2: The extent and nature of IT activity carried out in the program areas is fully transparent

2.4 General comments for Criterion 2

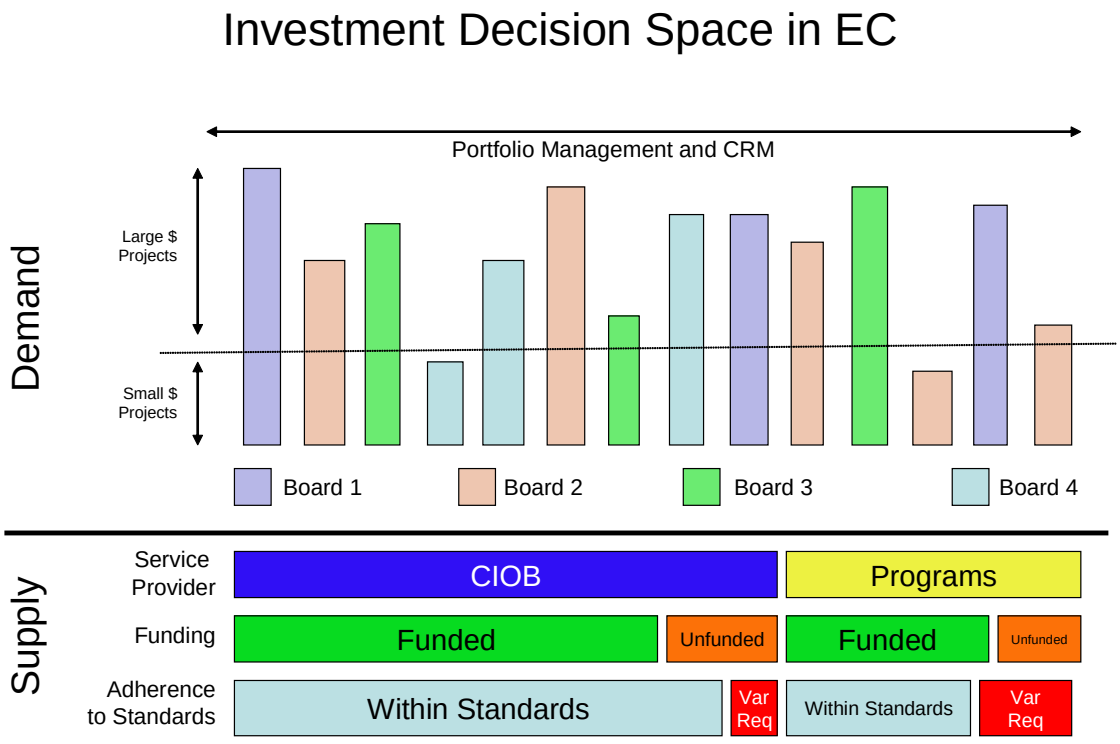


Figure 1: Decision space for IT Investments

When studying this criterion, we expected to find tools and processes for making a number of decisions that are critical to the efficient and effective use of IT resources. Figure 1 depicts some of the decisions that are considered when investing in IT activity. The figure shows the decision space split into demand-side decisions and supply-side decisions, as discussed in section 2.2 above. The decisions required in the demand-side revolve around what activities will proceed and which ones will not. The issues surrounding these decisions are described in section 2.5 below. The first supply-side decision highlighted in the figure is who will deliver the IT services, and this issue is described in sections 2.6 and 2.9 below. Although the second supply-side decision is not dealt with in detail in this report, we note that the Department has moved to an "integrated planning" process for the 2010–2011 fiscal year that integrates financial, human resources (HR) and IT planning with project planning. The final supply-side decision depicted in the figure is whether the activity will be conducted according to agreed-upon departmental standards or whether a variance must be granted. This issue is discussed in more detail in sections 2.7 and 2.8 below.

2.5 The framework for investments does not always handle small projects or projects to maintain existing operations adequately, and it does not provide a mechanism for the resolution of IT demand conflicts that cross boards

We expected to find evidence of a framework for prioritizing IT investments and ensuring their alignment with business objectives. Further, we expected that this framework would accommodate projects of all sizes and that it would accommodate the delivery of both centralized IT services and centrally governed but program-delivered IT services. Finally, we expected to find evidence that decisions made according to this framework are communicated to both the project managers that initiated the project and to the CIO.

Figure 1 summarizes our findings from interviews and document reviews on the nature of the demand and supply-side decisions that are commonly required when carrying out IT activity. In the figure, the demand for IT service is found above the line and is represented as being a mix of large and small projects that have been proposed by program areas and regions. We found that this mix of projects is analyzed by the portfolio managers and CRMs to identify opportunities for meeting the needs with a minimum of redundant activity, and in a way that increases synergies across functions. When this analysis is presented to the boards, they make decisions about their areas of highest priority, and these priority areas and the accompanying analysis by the portfolio managers inform the investment decisions and allocation of resources made for the project mix in a given board.

We found that the framework for making decisions exists and works well for establishing the priority of large-scale IT investments within a given board and for determining what IT activity will arise from these priorities. We observed that managers and staff often identified their boards as being responsible for deciding which IT activities were approved. We also observed, however, that this understanding was more often expressed by managers of large projects than with managers of small-scale projects and projects to maintain existing operations.

We observed that, within this framework, boards establish priorities for investments in IT and that these priorities are communicated to CIOB. We observed that CIOB uses these priorities when deciding to which activities it must allocate its resources.

We also observed that, in fiscal year 2008–2009, the CIO implemented a portfolio management function to help the boards determine which IT investments would best ensure the alignment of IT activities with their priorities. We note that both COBIT and TBS consider portfolio management to be a best practice for ensuring alignment of business and IT goals.

We observed that portfolio managers have been made responsible for managing the demand side of the IT investment framework from a CIOB perspective. We also observed that as well as ensuring alignment between IT activities and Board priorities, they are responsible for portfolio analysis, i.e., for ensuring that IT expenditures in one area do not duplicate work being carried out in another area. We note that the analysis of synergies to be made across boards is restricted to those priorities that have already been established by the boards. We observed that there is no mechanism, short of going to the EMC, for optimizing value where there are conflicting priorities across two or more boards. CIOB has expressed frustration with this situation.

We observed that while program managers and staff working on approved development activities frequently reported that their boards were responsible for the decisions to invest in their IT projects, managers that had unsatisfied requirements (often those responsible for small-scale projects or projects to maintain existing operations) often reported being unsure of who made these investment decisions or the reasons why their projects did not get approved. We observed that these managers often attributed the negative decision to CIOB rather than to their board or to the management of their program. They also more often reported not knowing what process to use to have their project approved or, when they knew what process to use, they reported that the process was too onerous for the amount of work they required.

When interviewing regional program managers, we found instances where their IT priorities did not seem to be aligned with national program priorities. This may be evidence of an incomplete transformation from the regionally delivered services model to a nationally delivered services model. In one example, we observed that a regional manager had requested some database maintenance to allow the region to continue to comply with an existing federal-provincial agreement, and that CIOB had responded that it was not in a position to address the needs because they were not aligned to priority areas identified by the board in question.

This raises the issue of how the boards and program management are communicating their investment and prioritization decisions to their managers and staff. During fieldwork we found no evidence of documented processes for sharing these investment decisions with managers and staff. We observed, however, that a CIOB portfolio management Ecollab site has recently been created (one that is accessible by all staff in the Department); it reports the status of all registered requests for IT activity being considered by the boards. We note that it is unclear how, or whether, this process will affect smaller projects that are never reviewed by the boards.

Aside from information that the CIO might gain as a member on various boards and committees, we found no evidence of a mechanism to ensure that investments made directly by the program areas in IT activity would be reported to the CIO. On the other hand, we note that although the CIO does present the boards with a summary of expenditures (dollars and full-time equivalents) for development projects, we saw no evidence of reports by the CIO describing how monies were spent in support of the Department's IT infrastructure and in support of operations. This finding was supported by the executive of one of the program areas, who noted that reporting by the CIO on how IT resources are being spent is largely project-based and does not go into sufficient detail about what investments are made to keep current operations functioning.

2.5.1 Impact

Without a mechanism for reporting, to the CIO, all the IT activity that is carried out in the program areas, the CIO will not be able to provide EMC or the Office of the Comptroller General of Canada with a complete picture of IT expenditures. This will reduce the ability to make decisions about how to best align IT activity with priorities, and may make the Department non-compliant with the Directive on Management of Information Technology.

Furthermore, without a mechanism to inform the CIO about the entire extent and nature of the activity being carried out in the program areas, applications will likely be developed without the knowledge or oversight of the CIO. In this instance the CIO would be unable to ensure adequate governance of these activities in regard to adherence to

standards and architecture, thereby placing the Department's IT security in question and making the resulting applications more difficult to maintain. It is also more likely that work conducted without CIO oversight will duplicate work already being carried out in other areas of the Department. In addition, this situation may reduce the CIO's ability to find efficiencies in IT processes that could be reinvested in other program priorities.

If the boards do not communicate their decisions about IT priorities and resulting investments back to the originators of the requests for IT services, managers of unsuccessful projects may attribute these negative decisions to CIOB rather than attributing them to their board. This, in turn, may lead to general dissatisfaction with the level of service provided by CIOB and the belief that it is better to do the development "under the table," undermining the potential for reinvestments resulting from the optimization offered by the CIO model. Furthermore, and perhaps of greater long-term importance, this situation may mean that the boards and program areas miss the opportunity to reinforce in the minds of their managers the operational priorities that they have established.

Having no mechanism to address competing demand for IT resources between boards means that high priorities from one board might not be met because the board does not have sufficient resources to allocate to them, while another board is able to address priorities of lesser importance because it has more resources available. This may lead to instances where IT resources are allocated to projects in such a way that the return on investment for the Department as a whole is not optimized.

When considering the way that IT investments are reported to the boards, if program ADMs and boards do not receive sufficient information about how IT resources are being spent in support of ongoing operations, they may not be in a position to provide adequate direction on current priorities. This may result in investment decisions being made that ignore or attribute the wrong value to IT investments made in support of ongoing operations.

2.5.2 Recommendations

3) The CIO, in consultation with EMC colleagues, should ensure that adequate mechanisms exist for making IT investment decisions (including investments for ongoing operations and investment decisions for embedded IT staff and their associated activities) in the new integrated planning process. The resulting plan should be presented to EMC for ratification of cross-board priorities and for approval.

4) The CIO, in consultation with the ADMs responsible for program delivery and with the assistance of the CFO, should develop better tools for reporting the expenditures made in IT. These tools should give the boards and EMC a complete breakdown of all expenditures in IT, including those required for the maintenance of the infrastructure and operations, and they should allow branch ADMs to report on the extent and nature of all IT activity being carried out in the program areas so that the boards and EMC can review the investment decisions that have been made.

2.6 No official criteria exist to decide when program areas should carry out IT activities independently

Given the scientific nature of the Department, it was expected that we would find IT staff with highly specialized skill sets embedded in the program areas.

We expected to find a well-communicated framework for making decisions about when it is appropriate for program areas to use their resources to deliver IT services rather than having those services provided by CIOB. Nominally, this would include a set of criteria to help program managers make this decision, but the framework might include procedures and tools to support the decision-making process.

We further expected to see evidence that these decisions were made at a management level, were well documented, and were reported to the CIO.

We found no official criteria that could be used by program managers to decide whether to have IT services delivered by CIOB or their own staff.

We observed that, in the absence of official criteria, program managers are making this type of decision according to criteria established on a case-by-case basis. Program managers reported considering project time frames, the available budget, agility (flexibility and adaptability), availability of resources, the overhead imposed by CIOB processes, and the requirement for specialized skill sets not available within CIOB when making these decisions.

We noted that the embedded IT staff who were interviewed included developers with highly specialized scientific skill sets and those with more generic IT skill sets.

2.6.1 Impact

Without a framework for deciding when it is appropriate to use embedded resources to perform IT activity, program areas are left to determine the criteria on their own, often on a case-by-case basis. As a result:

- there is a possibility that IT activity will be conducted “under the radar” without oversight by CIOB. As oversight by CIOB is meant to ensure that the activities are adequately governed, this in turn increases the chances that development activities will be inconsistent with departmental architecture and standards and will be more costly to maintain over time;
- the Department may miss out on the opportunity for reinvestment that optimizing IT expenditures can provide.

2.6.2 Recommendation

5) The CIO, in consultation with the ADMs responsible for program delivery, should create criteria for deciding when it is appropriate for program areas to carry out IT activity. Once created, the criteria should be presented to the EMC for approval.

2.7 Architecture, processes and standards are not effectively communicated

We expected to find an architectural vision for IT in the Department, supported by documented processes and standards. We also expected to find evidence that this architectural vision (and the associated procedures and standards) was widely communicated throughout the Department.

We further expected to find evidence of processes to allow stakeholders to have input on: the architectural vision; the creation of new standards; and the refreshing or decommissioning of obsolete standards, as well as a mechanism for obtaining a variance to the departmental standards (when such a variance is required to meet departmental objectives and does not have a negative impact on the departmental architecture and infrastructure).

In addition, we expected to find a mechanism to ensure that development within the program areas is monitored to ensure that it adheres to the architectural vision, except as amended by granted variances.

We found evidence that CIOB has an Enterprise Architecture (EA) group supported by a governance committee structure, including an EA board supported by an EA committee and four EA subcommittees. This group is developing an architectural vision for the Department in four major areas: business architecture, information architecture, application architecture and technical architecture. These four sub-architectures are supported by a horizontal IT security architecture. The EA group acknowledges that they are currently at a low level on the maturity curve,[*] but they have developed a strategy for climbing the maturity curve over time and are implementing this strategy.

We observed that, although clients are allowed to contact members of any of the architecture committees, membership on those committees and on the Architecture Review Board is restricted to CIOB staff, which tends to limit client influence over the selection of standards and over architectural direction.

During interviews and document reviews we found that the EA group's intent is to allow the EA to mature over time, while allowing other groups that are farther ahead (in some respect) to continue their work as the architectural vision of the Department catches up. In this regard, we also noted that program areas often conducted their IT activities according to agreed-upon international standards (such as those specified by the World Meteorological Organization) or standards imposed on them by third parties such as the Department of National Defence and other client departments.

We observed that the architectural subcommittees and work groups for the four major sub-domains met regularly last year, and made a number of recommendations that were eventually presented to the Architecture Review Board for approval. We also observed that architectural decisions are being made and documented by the Architecture Review Board.

We observed that the EA group was in the process of creating a repository of standards (both those that are approved and those that are still under consideration) that have been historically used within the Department. We note that this repository is still a work in progress and does not capture all of the standards currently employed within the

[*] Architecture Capability Maturity Model as of July 9, 2010, CIOB

Department. We observed that the repository has only recently been published on a collaborative web site that is open to the IT community outside of CIOB.

CIOB recently hosted a meeting of embedded IT staff, during which embedded staff were invited to bring forward, for consideration, standards that they were currently using when carrying out their work. The process to accomplish this was not articulated at the meeting, and we found no evidence of a written process for amending the list of standards or for obtaining a variance from the standards when required to meet business objectives.

We found no evidence of any departmental policy or directive that would require program-delivered specialized IT activities to be conducted within the Department's architectural vision or standards (as amended by authorized variances). We observed that it would be difficult for CIOB to discover the extent and nature of the IT activity that was being carried out by the programs. We also found no evidence of processes that CIOB could use to monitor specialized IT activities that it was aware of, in order to ensure the provision of adequate oversight.

2.7.1 Impact

Without an adequately defined and communicated architecture and established standards, applications that are developed will work together, at best, by accident. In the worst case, these applications may compromise the security of the enterprise or the activity of existing applications, thus putting the achievement of departmental goals at risk.

However, even if an architectural vision is available (either partially or completely), it will provide little value to the organization unless it is widely and effectively communicated to the people responsible for carrying out the work.

Standards must be able to adapt to changing business needs and to take advantage of advances in technology. Not allowing the program areas to influence the selection of standards, and not having a process to obtain variances from published standard, may lead to: lost business opportunity; failure to meet program goals; or the proliferation of under-the-radar development with no standards or with "home-grown" standards that are not consistent with the departmental infrastructure.

Additionally, if the architecture and standards are not well understood, the ability to reuse code or redeploy resources may be limited, thus reducing efficiency and causing lost opportunity for reinvestment in areas of higher priority.

2.7.2 Recommendation

6) Building on the strong work already being undertaken as part of the transformation of CIOB in the areas of architecture, processes and standards, the CIO should, in consultation with the ADMs responsible for program delivery, establish mechanisms to engage programs/clients in developing, broadly communicating, and publishing EC's Enterprise Architecture Vision, processes and standards. This would include program area participation as members of the Architecture Review Board.

   Further, the CIO, in consultation with ADMs responsible for program delivery, should establish and implement mechanisms for appropriate oversight,

monitoring and reporting of IT activity, to assure compliance with standards and optimal use and investment of IT resources.

The CIO, in consultation with ADMs responsible for program delivery, should establish an IT resource "blueprint" comprising competencies, knowledge and skills standards, and training and learning.

2.8 Central repository of information about departmental data does not exist

As our audit scope was restricted to dealing with the governance of Crown data assets (and especially scientific data sets), our expectations were limited to finding an enterprise data management program, including an inventory of Crown-owned data assets that describes, at a minimum, the nature of the data that are being captured, the purpose of the data, the custodians of the data, and the location of the data sets.

We also expected to find that data identified in the inventory were stored on enterprise-level servers that have adequately-implemented security as well as adequate backup and recovery capacity.

Although we found examples of excellent data management practices in the program areas (such as the data management initiative), we noted that there is no comprehensive inventory of data assets maintained by the Department. Without this inventory, it was not possible to test how well our corporate data are stored and protected.

We noted that the Data Management Framework was jointly created by a co-operative initiative involving the Information Management Directorate in CIOB as well as the Meteorological Service of Canada (MSC). This initiative is meant to store data and metadata for MSC operations. Other initiatives exist to document data being captured by various parts of the organization.

We heard a large amount of anecdotal evidence indicating that not all Crown data were being stored on enterprise-class servers.

We found that most of the servers that were originally owned and maintained by the program areas are now under the control and management of CIOB, and are housed in secure locations. These servers are backed up on a regular basis.

We saw no evidence that CIOB is aware of what data are stored on each of the servers they maintain for the program areas, including whether that data is critical to meeting departmental objectives and who to contact for more information about the data. We note that CIOB reported that they have an ongoing project to identify, and bring under CIOB governance, the remaining "under the desk" servers in the Department. We also note that the hardware acquisition process was changed to require CIOB involvement in the acquisition of any computer equipment, meaning the problem of "rogue" servers should disappear over time.

2.8.1 Impact

Being a science department, our data are critical to our ability to deliver on our priorities and objectives. Whether it is the provision of real-time weather data, the maintenance of a long-term time series of pollutants in the atmosphere, or one of our many other scientific functions, our data are critical to the science we carry out on behalf of

Canadians and the environment. Although individual data sets may be well documented, not having a departmental inventory of data that have been captured and that are being maintained may lead to situations where we capture the same information more than once because we are unaware that we already have it; we are unable to respond effectively to access-to-information requests; we do not make the best use of information assets that we already maintain; and in the worst case, we lose access to the information entirely, through system failure or due to the departure of the data custodians.

2.8.2 Recommendations

7) The CIO, in consultation with EMC colleagues, should establish an enterprise data management program that includes, as a minimum, a sustainable centralized inventory of Crown data under the custody of the Department. This inventory should include (but not be limited to) information about: the nature of the data that is held; the volatility of the data; the source(s) and location(s) of the data; the contact information for the appointed steward of the data; and the criticality or sensitivity of the data.

   This centralized inventory (corporate metadata repository) should be the system of record for departmental metadata, and departmental processes should be established to ensure that appointed data stewards create and maintain the metadata for all data of business value. Data producers, consumers and data management systems across the Department should reference and update this corporate metadata repository when inquiring about the existence of departmental data.

8) The ADMs responsible for program delivery should ensure that all departmental databases under the control of their branch are represented in the corporate metadata repository.

2.9 Criteria and procedures to determine when it is appropriate for program areas to staff IT positions are not adequate

We expected to find that the staffing of all positions that carry out IT activity would respect criteria agreed upon by all parties and that the staffing process would involve oversight by the CIO. We expected that this would include positions designated as CS positions and positions with other classifications where a significant amount of the workload is IM- and/or IT-related.

Further, given that one of the major reasons stated for having IT staff in the program area was the specialized skill sets necessary to carry out their work (such as advanced math degrees or other science education or experience), we further expected to find succession plans for all IT positions that required a specialized skill set.

We found that the oversight by the CIO for the staffing of CS positions is effective. We found one example of non-CS positions being staffed where the job description clearly indicates that the incumbent will be doing largely IT-related activity, and we heard anecdotal evidence from CIOB staff that this was not an isolated occurrence. We found that no mechanism exists to ensure that the CIO can provide oversight over the staffing of these positions. We were told by CIOB staff that this type of staffing is occasionally carried out to bypass oversight by the CIO. We were also told by a senior program

manager that if they felt the need to have someone in another classification do IT work, it was within their prerogative to do so.

Although we found considerable evidence of specialized skills among CS staff in the program areas (with some IT staff having PhDs in math or other sciences), we also encountered a number of CS staff in the program areas who perform more or less generic IT activities.

When speaking about succession planning for scientific programmers, we were told that in some cases it can take four or more years in a position before a candidate masters their area of activity, and that the skill sets for one position do not necessarily translate into those required for another scientific position. The implication here is that one must work in the position for a number of years before one is able to perform the required tasks fully, which further implies that it is necessary to bring replacements in before staff with specialized skill sets retire. Because it can take four years before a new employee becomes fully capable of replacing a departing employee, the replacement process must be continuous. We were told by one senior program executive that if they needed to find a replacement for their more specialized staff, they would turn to their international colleagues in weather services rather than to CIOB, because weather services would be more likely to have someone with the appropriate skill set. Although we did not see any evidence of a list of potential candidates from the international community for any of our specialized IT resources, it is reasonable to assume that managers of scientific staff are aware of the identity of potential candidates.

We found that the branch HR plans for the three most-affected branches do deal with succession planning for individuals with highly specialized skill sets. Of the three, the HR plan of the most-affected branch (Science and Technology) has a number of concrete actions that they are taking or plan to take to address this concern. The HR plan for MSC also states that “Skills shortage may be more prevalent among certain occupational groups. To respond to this reality in the scarcity of experts, the MSC People Plan aims at building our people capacity through recruitment, training and succession planning.” The plan also describes a pilot project that MSC is conducting to address the issue.

During interviews, program managers also told us that their strategy has been to hire co-op students, and to bridge the best of these into permanent positions at the end of their co-op program.

We found no evidence of a competency inventory that would allow management to determine what skills in the organization were so specialized that there would be a threat to the Department in the event of the loss of an employee. We did not ask to see examples of succession plans for specific individuals, and we believe that this should be the subject of any future audit or review of succession planning.

The CIOB IM & IT HR strategy for 2009–2010 also speaks about succession planning at a very high level. It lists the priority areas for staffing in terms of: having the adequate mix of people and skills; having an organizational structure to meet the objectives and priorities of the organization; having best practices for wellness, work-life balance and workload issues; and encouraging learning and development in terms of providing the adequate training for staff to be successful in their roles. This strategy is only aimed at the CS community within CIOB and it does not significantly indicate how CIOB intends to accomplish these strategic goals.

Finally, none of the embedded staff that we interviewed could remember receiving any training in IT practices in the previous three years, and very few of them reported receiving any guidance from CIOB.

2.9.1 Impact

Without sufficient oversight in the staffing process for IT positions, the CIO may be unable to provide adequate governance for IT activities—including adherence to the departmental architectural vision and standards. This may lead to: instability in the departmental infrastructure; security gaps; applications that are difficult and costly to maintain; applications that do not reuse code effectively; and possible problems with licensing or Crown copyright of applications.

Staffing of new IT positions, whether in CIOB or the program areas, brings with it ongoing liabilities (salaries, pensions, accommodations, etc.), and if it is undertaken to deal with short-term capacity problems alone, the ongoing liabilities this staffing implies may put the Department into a position where it cannot take on new opportunities due to lack of resources.

Given the highly specialized skill sets of many of our specialized IT staff, failure to do succession planning for specialized IT resources may expose the Department to a serious risk that it would not be able to provide continuous services in support of its mandate. The HR plans for the three most-affected program areas indicate that those areas are fully aware of the issue and are taking meaningful steps to mitigate the risk. We believe that not having a competency profile for all positions requiring specialized skill sets increases the level of risk to some degree.

Additionally, not having access to training may affect the career path for IT personnel in the program areas, which may lead to recruitment and retention issues and cause future problems for succession planning.

2.9.2 Recommendations

9) The CIO, in consultation with ADMs responsible for program delivery, should create criteria for deciding when it is appropriate for program areas to staff IT-related positions. The criteria should:

- clearly define the scope and nature of the roles these staff will play, and define the functional relationships that these staff will have with the CIO;
- be accompanied by directives and guidance on the use of architecture, standards and procedures for conducting the IT activity.

10) The CIO should ensure that newly hired IM and IT employees receive mandatory orientation on standards, architecture and IT processes. Further, the CIO should ensure that CIOB places no impediments in the way of embedded IT staff attending any IT training that is available to CIOB staff.

11) Program ADMs responsible for specialized IM and IT personnel should:

- ensure that branches develop specific succession plans for each employee (or group of employees) who has a specialized skill set that is necessary to carry out a given job;

- ensure that employee training and development plans for embedded IM and IT staff include training on departmental architecture, standards and processes; and
- ensure that specialized IM and IT activities are carried out by properly qualified staff.

3 CONCLUSION

Based upon an analysis of our observations and the evidence we received during the audit, we conclude that the current overall level of governance for specialized IT is not yet adequate, and that a number of changes are required to allow the maturity level to rise to an adequate level. Accomplishing these changes will require the co-operation of all parties with an interest in the governance of IT activities in the Department.

4 MANAGEMENT RESPONSE

CIOB RESPONSE

Overall, CIOB accepts the observations, findings and recommendations of the Audit of Governance of Specialized IT Resources, which reflect a lower level of maturity for IM & IT governance within EC.

Current and expected future fiscal constraints make it timely to revisit, review and update EC's associated management structures and supporting processes, in order to provide EC executives with the insight and information required for assurance of optimal IM & IT resource investment decisions in service to EC strategic imperatives and program priorities.

CIOB's three-year IM & IT plan, 2010–2011 business plans, and program of work are consistent with and address maturity improvements in many of the recommended areas to be addressed in this audit, with the pace of implementation subject to budget allocations and resource demands.

In considering the audit report's recommendations, CIOB's management action plan takes the following key factors into account:

- Current program/client and CIOB maturity levels
- Resource investment required to accelerate the rate and pace of the Department's maturity to recommended levels
- Relative level of risk and exposure associated with current maturity levels related to the above[*] versus other levels of EC risks and exposure

The CIOB Management Action Plan contains four components that address the recommendations outlined in the audit report. Please note that completion dates are subject to consultation on the Management Action Plan with programs/clients, and on confirmation of CIOB's 2010–2011 budget allocation.

METIOROLOGICAL SERVICES OF CANADA RESPONSE

With respect to recommendation 8 the success of this recommendation is contingent upon guidelines that should be developed by CIOB, e.g. a document that describes the

[*] "the above" refers to the relative risks arising from the audit reports recommendations

departmental metadata repository and provide guidelines to Branches regarding what should be included in the repository. That said, the MSC will continue to work with CIOB in supporting sustainable, accessible and robust data management approaches.

MSC collects and manages large volumes of near real time, through to historical data, which are essential in delivering weather, water, air quality and climate related products and services. A robust data management framework is essential for ensuring that our business objectives are met. This includes our obligation to share meteorological and other data, with, for example, the World Meteorological Organization on an ongoing basis that conforms to international standards and approaches.

The MSC will continue to collaborate with CIOB on the development of the Data Management Framework and other approaches to oversee data management, such as the metadata repository. The Data Management framework will ensure the metadata required for this repository is available.

As well, the development and implementation of the Asset and Life-Cycle Management system will ensure that metadata reflects and supports life-cycle management of the networks.

With respect to recommendation 11 the MSC People Plan focuses on succession planning, training, and retention of all MSC employees, including the specialized IM/IT resources. In particular:

- Ensure that branches develop specific succession plans for each employee (or group of employees) that has a specialized skill-set that is necessary to carry out a given job.

Within the MSC there are two main areas where specialized imbedded CS resources are essential in contributing ongoing specialized expertise to support core program outcomes; both within the Weather and Environmental Prediction and Services Directorate.

Recruitment of the required experts, training, and succession needs are of key concern to the operational success of the environmental prediction system (which includes an in-depth understanding of the numerical weather prediction model suite and science; international modeling science, advanced and complex data stream management and; interfacing with complex informatics systems, as well as understanding the desired science program outcomes for example the air quality index or new marine program products).

It takes years to develop this combination of expertise and is largely developed through the work environment once hired. The MSC will continue to ensure that the appropriate on the job training takes place to retain and develop our embedded CS experts. It should be noted that turn over in these Division is much lower than the EC average, making it even more important that the Directors ensure that their staff career development is fully supported, and managed.

With this in mind, the Prediction Development Division and Prediction Operations Division are currently developing Human Resource plans which focus on the evolving needs of the Divisions, including the CS' who work in each Division.

- Ensure that employee training and development plans for embedded IM and IT staff include training on departmental architecture, standards and processes

MSC will work with CIOB to ensure that both Branches have a common understanding of the existence of training materials, standards and processes and its accessibility to all EC CS staff.

In the absence of existing material, the MSC will rely on the CIO Branch to develop and provide consistent training material to the MSC. When official Departmental training exists, and is offered to Branch staff, MSC will ensure that their CS' are trained on the departmental architecture, standards and processes that are implicated in their day to day work (as opposed to normal "run" oriented desk top operations).

- Ensure that specialized IM and IT activities are carried out by properly qualified staff."

MSC is committed to ensuring that the work of their CS' is high quality, meets program needs and respects standards. MSC will work with CIOB to define what is considered "properly qualified staff" in the context of the both program operational needs and CIOB governance goals.

SCIENCE AND TECHNOLOGY BRANCH RESPONSE

With respect to recommendation 8 S&T Branch agrees with this recommendation and will work with CIOB to ensure that departmental databases under our control are represented in the corporate metadata repository.

With respect to recommendation 11 S&T Branch agrees with this recommendation and notes that policies and processes are already in place to support their implementation.

The Branch is currently developing a leadership development and succession planning framework to ensure that the Branch is able to recruit, develop and retain capacity in key areas. We will look at using this framework, as well as other succession planning activities in the Branch to meet this recommendation.

S&T Branch will have in place learning plans for all its employees, and the Branch will work with CIOB to ensure that the recommended elements are included in the training and development plans of embedded IM/IT staff.

The Branch continuously works with HR to maintain a high quality in our staffing processes to ensure we are employing highly qualified staff.

ENVIRONMENTAL STEWARDSHIP BRANCH RESPONSE

With respect to recommendation 8 we will get a complete list of departmental databases that are under ESB control and determine who the responsible DGs are.

Ensure that any relevant databases in ESB are represented in the corporate metadata repository.

With respect to recommendation 11 we will, as a first step, get a complete list of all CS positions, if any that are within ESB control and to which DG they report to.

Determine what is the specialized skill set required for the position(s). Ensure that the position(s) requirements is/are carried out by properly qualified employee(s) and determine if additional training is required

Make certain that employees in these positions have the sufficient training on departmental architecture, standards and processes. If not, ensure that they take any necessary training.

Annex 1
Audit Criteria

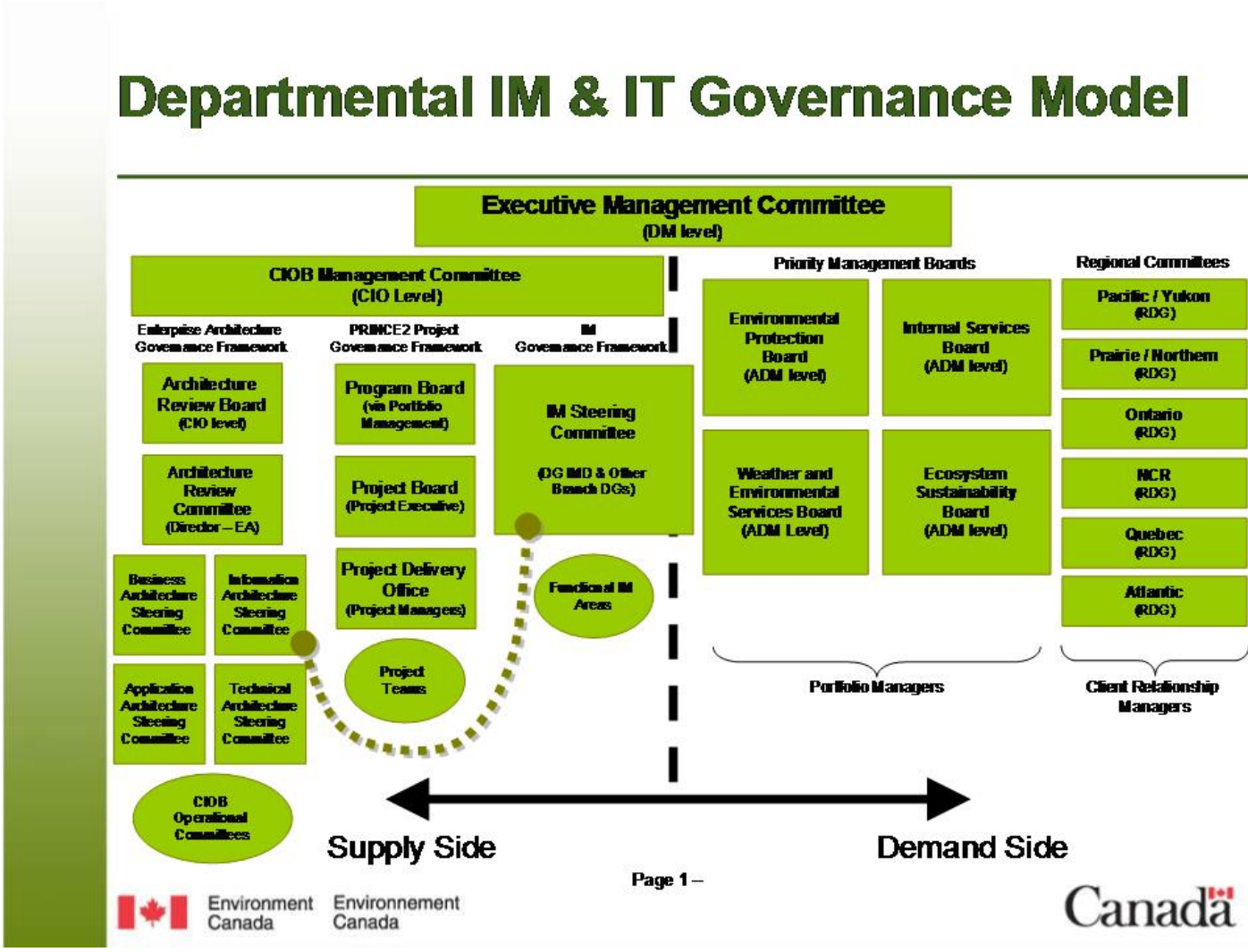
The criteria for this audit have been adapted from the COBIT 4.1 framework for IT governance. Specifically, they relate to control objectives found in the chapter "ME4 – Provide IT Governance" and the "PO Plan and Organize" chapters. The wording of the criteria has been modified as necessary to respect the scope of the audit.

1. Roles and responsibilities of the players responsible for the governance of specialized IM and IT activities are well articulated and understood.
2. The extent and nature of IM and IT activity carried out in the program areas is fully transparent:
   a. Value-delivery objectives are assured by demonstrating that decisions about which resources to use for development projects have been clearly articulated and reported to the CIO.
   b. Resource management objectives are assured by demonstrating that expenditures on IM and IT activities and IT acquisitions were fully documented, are aligned with business objectives, and take advantage where possible of pre-existing infrastructure and code.
   c. Resource management objectives are also assured by demonstrating that processes exist to consistently identify and describe the scope and nature of Crown-owned information assets being created or maintained by the Department.
   d. Resource management objectives are further assured by demonstrating that staffing decisions are made following a well-defined logic model and are subject to oversight by the CIO.
   e. Resource management objectives are further assured by demonstrating that succession planning is undertaken for positions requiring specialized skill sets.
   f. Performance measurement and strategic alignment objectives are assured by demonstrating that processes and standards for governing the IM and IT activity were documented and followed.
   g. Performance measurement and strategic alignment objectives are further assured by having a process to establish priorities for IT expenditures that is transparent and involves all stakeholders.
   h. Risk management objectives are assured by demonstrating that: processes exist and are followed to assess the criticality of the applications/solutions that result from specialized IM and IT activity; business continuity plans are created for systems that deliver critical services; and the results of the assessments and the business continuity planning are reported to the CIO.
   i. Risk management objectives are further assured by demonstrating that processes exist to identify and mitigate risks arising from IM and IT activity, and unmitigated risks are documented and accepted by management and reported to the CIO.
   j. Independent assurance objectives are assured by demonstrating that quality assurance processes exist for specialized IM and IT activities.

Annex 2
List of Background Information and Supporting Documentation

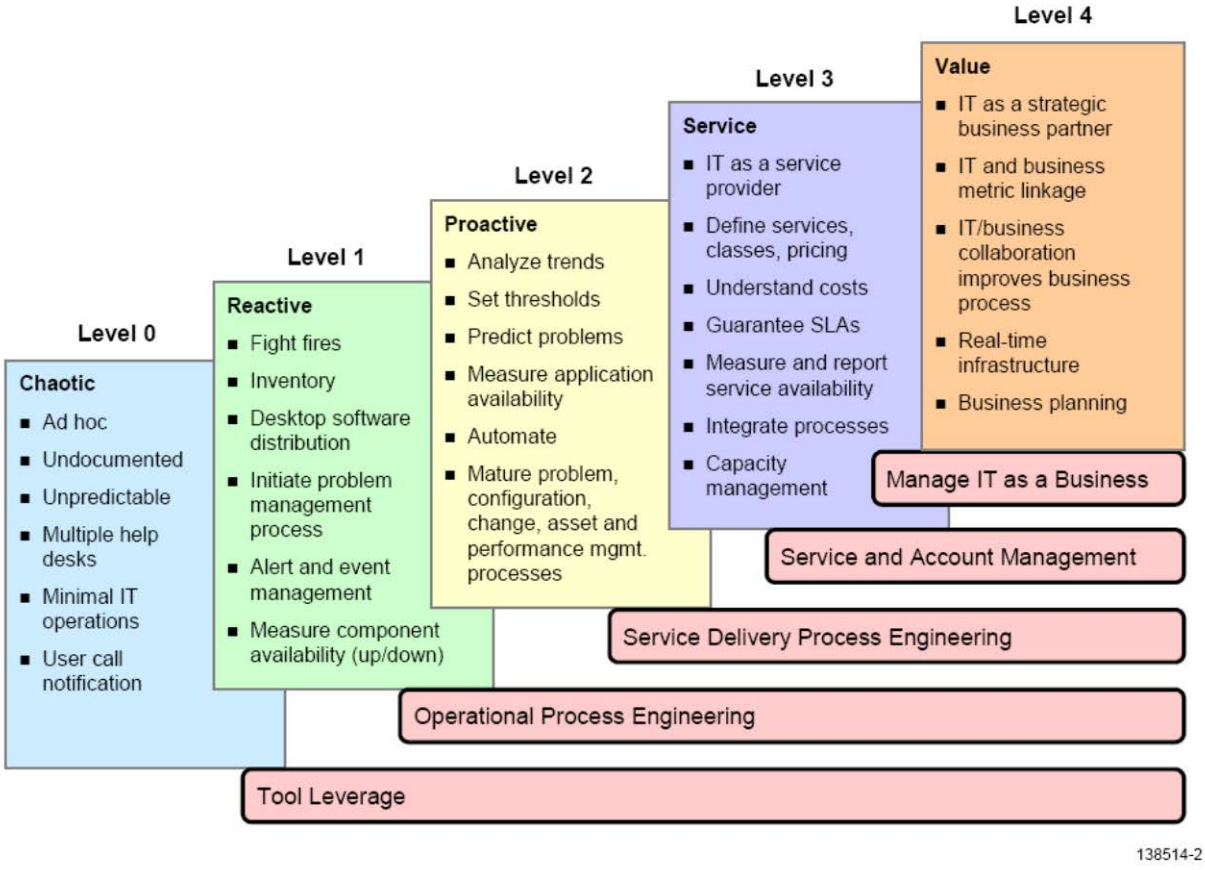
Intentionally Blank

Annex 3
Draft CIOB IM and IT Governance Model



Annex 4
Maturity Levels

(Source: Gartner Inc., April 2006)



Source: Gartner (April 2006)

Annex 5
Acronyms and Terms

ADM	Assistant Deputy Minister
CIO	Chief Information Officer
CIOB	Chief Information Officer Branch
COBIT	Control Objectives for Information and related Technology (a control framework for the governance of IT)
CRM	Client relationship manager
CS	Computer systems (refers to employees who are staffed in positions classified as part of the CS group and whose primary job is in IM and/or IT)
data	For the purposes of this audit, "data" has the most generic sense. The scope of the audit was restricted to looking at any scientific data that are captured, created or received by the Department and that are owned by the Crown. The requirements for storage of this data may vary by type; however, there are requirements, as outlined in the *Library and Archives of Canada Act*, related regulations, and multi-institution disposition authorities.
EA	Enterprise Architecture
EC	Environment Canada
EMC	Executive Management Committee
IM	Information Management
IT	Information Technology
ITIL™	"A registered trademark for a cohesive best practice framework, drawn from the public and private sectors internationally", ITIL is a registered trademark that stands for Information Technology Infrastructure Library. Its focus is on IT as a service provider using IT Service Management concepts. It deals largely with the later stages of development through implementation, and includes operations.
SLA	Service Level Agreement. This refers to a negotiated level of service to be provided by a service provider to a service consumer for a given price.
MAF	Management Accountability Framework
MSC	Meteorological Service of Canada
PAA	Program activity architecture is an inventory of all the program activities undertaken by a department. The program activities are depicted in their logical relationship to each other and to the strategic outcome(s) to which they contribute. The PAA is the initial document for the establishment of a management, resources and results structure.
Process	"The IT organisation delivers against these goals by a clearly defined set of processes that use people skills and technology infrastructure to run automated business applications while leveraging business information. These resources, together with the processes, constitute an enterprise architecture for IT"

	"COBIT defines IT activities in a generic process model within four domains. These domains are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. The domains map to IT's traditional responsibility areas of plan, build, run and monitor." (Source: COBIT 4.1 framework for IT governance.)
TB	Treasury Board
TBS	Treasury Board Secretariat
TTAC	Technology Transfer Advisory Committee
WES	Weather and Environmental Services
Run, Renew, Transform	This is CIOB's term for those activities that make up the full scope of IT activity in the Department, including those activities necessary to carry out daily business and maintain the operational infrastructure (run), those necessary to incrementally improve the Department's operations (renew), and those necessary to transform the organization and allow it to take advantage of synergies and streamline controls (transform).