Public Health Agency of Canada | Agence de la santé publique du Canada

AUDIT REPORT

ON THE INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY GOVERNANCE

Audit Services Division

September 2008

Approved by Chief Public Health Officer
on October 28, 2008

Canada

Table of Contents

Cat: HP5-76/2-2008E-PDF
ISBN: 978-1-100-10935-0

Executive Summary

1. The objective of the audit of the Information Management and Information Technology (IM/IT) governance was to assess the extent to which IM/IT at the Public Health Agency of Canada (PHAC or the Agency) uses appropriate IT governance principles. Appropriate IT governance principles are designed to enable IT to support the PHAC's strategic objectives and to ensure that IM/IT systems and processes effectively support the management and professional information needs of PHAC in a well controlled environment.

2. The audit examined PHAC IM/IT governance strategies and activities from April 1, 2007 to March 31, 2008. The IM component addressed in this report focused specifically on electronic data management and excluded the record management function.

IM/IT Management Framework

3. We noted that the Chief Information Officer (CIO) is not a member of the Executive Committee (EC). The inclusion of the CIO as an EC member would be consistent with international best practices.

4. The EC provided strategic orientations and provided direction to the Office of the CIO or direction on the alignment of the IM/IT's strategies and their related investments with the Agency's priorities.

5. PHAC's present governance committee structure does not include a committee dealing specifically with IM/IT issues. In general, an IM/IT committee would review and resolve issues specific to IM/IT across the Agency.

6. We noted that, although programs have managed the Surveillance activities, these activities were not specifically included in the IM/IT Strategic Plan. We believe that the absence of references to major program operations, such as Surveillance activities, and the absence of specific quantitative measures directly related to the objectives they are measuring could result in inadequacies to sustain the Agency strategies and objectives.

7. The Office of the CIO has not yet established a formal process for the development of its Strategic Plan. The implementation of a formal governance framework would result in coordinated efforts, greater transparency, effective risk management, timely communications, effective use of resources, and professional accountability.

8. There are many legacy HC IM/IT policies still in place at PHAC. This need to be reviewed and updated to reflect the Agency's new environment, and

evolving technology.

9. Traditionally PHAC programs have been responsible for the management of their IM/IT activities. In some cases, program IT staff have implemented their own infrastructure, acquired the technologies, assets, support from vendors, and contractors that they needed to accomplish their work without coordinating these activities with the Office of the CIO. This practice is sub-optimal, and exposes PHAC to undue risk that systems may be developed, or administered without appropriate risk management and control, or attention to the effective use of scarce resources.

IM/IT Resource Management

10. We observed numerous transfers of IT staff from HC to the Agency at all levels, which indicates that PHAC can attract new employees.

11. The IM/IT Directorate has reported to the Office of the Chief Financial Officer (CFO) that it does not have a budget sufficient to support the services and infrastructure that it is expected to manage for its clients within PHAC and faces shortfalls in Operation and Maintenance allocations.

12. The Agency does not have an approved multi-year budget allocation for IM/IT. Without such budgets, the IM/IT cannot adequately plan for the three-year hardware replacement, an industry best practice.

Acquisition of Automated Solutions

13. The large demand for new software and the lack of funds have resulted in numerous application developments being indefinitely postponed. In such circumstances, clients opt for alternative solutions such as third party developers or the acquisition of “off the shelf” software. These solutions are not optimal since “off the shelf” software often requires extensive customization at the time of implementation.

14. The IM/IT Directorate has requested from HC, without any success, sets of metrics that would provide insight into the outcomes and performance of the processes managed by HC.

Information Security Governance

15. We noted that PHAC has a low tolerance for risk while HC and PWGSC have a medium tolerance. The result is that when PHAC networks with HC or PWGSC systems it is exposed to greater risks than is desirable.

Acquisition, Safeguard, and Disposal of Electronic Data

16. Where IM services are available, they are not necessarily aligned with

Government of Canada standards and do not meet policy requirements in terms of identification, classification, retention and disposal. Employees and management across the Agency do not always understand policy requirements or the importance of good information management practices. Consequently, information is not safeguarded, managed, and disposed of effectively or efficiently.

17. The CIO does not currently have the required authority and resources to enforce standards or to measure enforcement and/or compliance with Treasury Board and PHAC requirements for acquisition, safeguard, and disposal of electronic data.

Conclusion

18. Established less than four years ago, PHAC has made some progress in building its IM/IT governance. The EC provided strategic orientations and direction to the Office of the CIO. However, there are several key areas where improvements need to be made. The improvements will enable IT to support the PHAC's strategic objectives and will ensure that IM/IT systems and processes effectively support the management and professional information needs of PHAC in a well controlled environment.

19. Key areas requiring improvement include:

- Provide regular updates on IT management to EC;
- Establish an IM/IT committee;
- Align IM/IT Strategic Plan with the Agency's Strategic Plan;
- Formalize and document the IM/IT strategic planning exercise;
- Review and adapt existing HC IM/IT policies;
- Renegotiate the provisions of the MOU with HC that relate to IM/IT;
- Review the level of IM/IT funding;
- Implement a multi-year budget allocation for IM/IT;
- CIO to approve all IM/IT acquisitions of hardware and software;
- Implement an internal IT change management process, with appropriate authorities;
- Review security risk tolerance levels; and
- Enforce Government of Canada standards related to electronic data.

Management Response

20. The Agency's management agrees with our findings and recommendations and a management action plan is presented in Appendix B.

Background

21. The audit of the Agency's Information Management and Information Technology (IM/IT) governance was conducted in accordance with the Risk-Based Audit Plan for 2008-09.

22. The Public Health Agency of Canada (PHAC or the Agency) was formed from the Public Population Health Branch (PPHB) of Health Canada (HC) in September 2004. IM/IT activities were highly decentralized at the outset, with local programs within the Branch (and subsequently PHAC) managing their own IM/IT resources and communicating directly with stakeholders. Commencing soon after its creation, PHAC began working to develop a more controlled environment consistent with best practices in IT governance.

23. HC provides PHAC with IM/IT direct services, shared services, and corporate IM/IT infrastructure. These services are rendered based upon a shared services model. The level of service provided is based on the level of service that was previously provided to the PPHB of HC prior to the creation of the PHAC.

24. In May 2005, the IM/IT Directorate initiated a Transition Project which included:

    - Enterprise IM/IT governance; and
    - Enterprise IM/IT planning.

25. It was considered desirable to manage the transition of the solution development and support functions within the IM/IT Directorate towards a centralized state that would reduce overlap. In early 2006, the Transition Project was redefined as an IT governance project. In February 2007, the EC approved the IM/IT Strategic Plan and the IM/IT governance model.

26. The IM/IT Directorate consists of 150 individuals providing direct services to PHAC staff. These services include network and data centre support, desktop services, IT security, records and information management services, application development and support, client relationship management, web hosting and intranet support, business analysis in support of IM/IT projects and project management.

27. For 2007-08, PHAC IT expenditures represent approximately $28 million (including one-time funding of $9 million for Operation and Maintenance (O&M)). The total is made up of: IM/IT Directorate salaries - $9.8 million; O&M - $12.8 million; and payments under the Memorandum of Understanding (MOU) with HC - $5.4 million. Since not all IT expenditures in PHAC are made with the knowledge of the IM/IT Directorate, there may be additional significant IT expenditures that are not readily apparent. A

review of the 2007-08 financial statements did not so indicate, however, and we did not pursue the matter further.

28. In December 2007, the Executive Committee (EC) approved a Surveillance Strategic Plan which identified the following goals:

- Create, implement, and maintain a responsive governance structure and network systems for surveillance within PHAC and accessible to partners when applicable;
- Establish and maintain a constant transfer of information and knowledge for public health decision-making;
- Effectively manage and maintain internal/external partnerships, engage them in collaborative surveillance activities that support public health action; and
- Develop and maintain timely and relevant performance measurement activities aligned with PHAC priorities.

29. PHAC has been managing a number of surveillance activities that vary in scope and in the degree to which they encompass the full cycle of surveillance. The new Surveillance Strategic Plan is intended to ensure that effective and timely surveillance activities are carried out and that these activities will provide the data and support necessary for federal/provincial/territorial/local jurisdictions to track, plan for, and respond to, emerging public health issues. Of course, of primary importance, effective surveillance serves as an early warning of potentially serious and urgent public health events.

30. The Surveillance Strategic Plan will affect the IM/IT Directorate because the Plan involves providing more centralized control over surveillance activities, with a concomitant need for greater centralized control over the related supporting IT infrastructure.

31. During the planning phase, the audit team identified the following areas of risk associated with IM/IT governance:

- Shrinking IM/IT labour pool;
- Aging infrastructure and too little re-capitalization;
- Scarce financial resources; and
- Additional business and security risks from having many networks and data centres to manage and control.

As a result of the above risk factors, the audit team assessed the following audit components as high risk:

- Strategic direction;
- Achievement of objectives;
- Appropriate management of risks; and

- Responsible use of resources.

Audit Objective

32. The objective of the audit of the IM/IT governance was to assess the extent to which IM/IT at PHAC uses appropriate IT governance principles. Appropriate IT governance principles are designed to enable IT to support PHAC's strategic objectives and to ensure that IM/IT systems and processes effectively support the management and professional information needs of PHAC in a well controlled environment.

Scope of Audit

33. The audit covered PHAC IM/IT governance strategies and activities from April 1, 2007 to March 31, 2008. The IM component focused specifically on electronic data management and excluded the records management function.

Approach and Methodology

34. This audit was conducted in accordance with the Treasury Board (TB) *Policy on Internal Audit* and the Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing*, except that no external assessment was performed to demonstrate that PHAC's internal audit function complied with the IIA Standards and Code of Ethics.

35. Audit criteria and sub-criteria presented in Appendix A were derived from CobiT Quickstart (Control Objectives for Information and Related Technology) which are the CobiT methodology guidelines for small and medium sized organizations, the TB *Policy on Management of Information Technology,* and the TB *Guide on Strategic Planning, Tips and Advice for IM/IT Strategic Plans.*

36. The audit team used a combination of audit methodologies including: identifying and documenting relevant PHAC policies and procedures; reviewing and documenting preliminary information provided by IM/IT; interviewing managers and key personnel and requesting evidence as required; and documenting and describing key IM/IT processes and practices.

37. The audit work was conducted between May and July 2008.

Audit Findings and Recommendations

IM/IT Management Framework

Criterion: An IM/IT management framework exists for decision, direction, and accountability. This framework is well understood and accepted by PHAC managers.

38. Corporate governance, in a public sector agency without a board of directors, is a set of executive and senior management responsibilities and practices designed to provide the organization with strategic direction, policies and guiding values. Effective corporate governance in this context provides assurance that the organization's goals are achievable, risks are properly addressed and organizational resources are properly utilized.

39. As per the TB *Policy on Information Technology Management*, the Chief Public Health Officer (CPHO) is accountable for the effective management of IT within PHAC, including the implementation of IT spending decisions and ensuring appropriate, ongoing measurement of IT performance.

40. IT governance is considered an integral part of corporate governance. The functions of IT governance are similar to, and derived from, the corporate functions but with a specific focus on IT.

41. Generally, IT governance includes the organized framework of roles, responsibilities, policies, and methods that an organization uses to guide, direct, and manage its IT resources. IM/IT management is expected to exercise leadership to direct and control IM/IT operations toward the achievement of the organization's goals.

42. At PHAC, the Chief Information Officer (CIO) is responsible for developing and implementing strategies, policies, standards and guidelines and key performance indicators to improve service delivery, IM, IT, privacy and security. Through these activities, the CIO plays a key role in identifying and leveraging opportunities to improve the overall quality and value for money of service delivery and internal operations.

Involvement of the Agency's Executive Committee in IM/IT

Sub-Criterion: Senior Management provides IM/IT with direction and support on horizontal issues that relate to network architecture improvement, application development, and investment decisions that IM/IT could incorporate into its Strategic Plan.

43. The EC establishes the Agency's strategy and objectives. In doing so, the EC strives to ensure that the Agency's goals are achievable, risks are properly addressed, and organizational resources are appropriately

allocated and utilized. The EC provides direction to the CIO on major issues that relate to the management of the IM/IT function. We noted that the CIO is not a member of the EC. The inclusion of the CIO as an EC member would be consistent with international best practices.

44. The EC guidance and input is essential because IM/IT is a horizontal function that requires governance and integrated strategies that involve multiple areas and programs in the Agency (e.g. network architecture improvement, corporate application development, and investment).

45. In February 2007, the EC provided strategic orientations and direction to the Office of the CIO. The EC agreed on:

- The approval of the proposed governance structure, IM/IT Strategic Plan and three priorities;
- Priorities: IM/IT Directorate would move ahead immediately on the governance structure, identify participants for the various committees, and ensure the governance structure is engaged in IM/IT priority setting and decision-making;
- IM/IT governance structure would include membership from across various sectors within the Agency to balance innovation and connectivity with the mandatory governance requirements;
- IM/IT Directorate would establish linkages with key committees with business and financial planning; and submit plan for review to appropriate committees; and
- Given the high degree of alignment between health surveillance and IM/IT, IM/IT Directorate would be included in the working group for the health surveillance project.

46. At the time of the audit, the above structures as suggested by EC were partially developed. The report addresses these issues in the following sections.

Recommendation

47. The Executive Committee should obtain regular updates on Information Technology management from the Chief Information Officer.

Governance Committees and IM/IT Decision-Making Processes

Sub-Criterion: The Office of the CIO is informed of major IM/IT plans of the Programs and has the authority and resources to ensure that such plans are implemented in accordance with PHAC's IT governance policies.

48. The CPHO and the EC carry out their governance duties in collaboration with governance committees and sub committees that oversee critical

areas. The following committees report to the EC:

- Resource, Planning and Management Committee
- Surveillance Management Committee
- Heads-Up Committee
- Public Health and Policy Committee
- Risk Management Committee
- Human Resources Committee
- Evaluation Committee

49. We noted that the CIO participates in the following committees:

- **Resource, Planning and Management Committee:** Provides advice on the Agency's resource allocation, planning, budgeting, together with financial and asset management policies and activities;

- **Surveillance Management Committee:** Advises the EC on surveillance issues, promotes horizontal information sharing, and oversees implementation of the Surveillance Strategic Plan;

- **Heads-Up Committee:** Presents a debrief of executive decisions and direction, as well as portfolio priorities;

- **Public Health and Policy Committee:** Facilitates coherence and coordination on policy, programmatic and corporate issues; and

- **Risk Management Committee:** Ensures that the CPHO and the EC receive timely, high-quality information, and advice on emerging and ongoing issues that require a risk management response. This is under the responsibility of the Assistant Deputy Minister-Infectious Disease and Emergency Preparedness Branch (ADM-IDEP), and the Chief Financial Officer (CFO).

In our view, the participation of the CIO in these committees is appropriate. Participation provides numerous opportunities for the CIO to become informed on key issues that need to be reflected in the IT Strategic Plan.

50. The present governance committee structure does not include a committee dealing specifically with IM/IT issues. Partly to compensate for this, the CIO met with most Agency senior managers during the past year. At these meetings, the CIO reviewed the governance structure recently developed by IM/IT together with IM/IT strategic issues and took advantage of the opportunity to learn about program plans and activities that might affect the IT Strategic Plan.

51. In general, an IM/IT committee (which could be called the "IT Governance Steering Committee") would review and resolve issues specific to IM/IT

such as setting IM/IT priorities in the Agency, establishing client service levels, recommending IM/IT financial and human resources allocation requirements to the EC, standardizing network and data architectures, establishing consistent and effective protocols for application development, priorizing short-term and long-term investment plans, supporting efficient and economical IT procurement policies and hardware standards, establishing effective IT security protocols and any other strategic matters. Such a committee could also facilitate decision-making for major IM/IT projects, keep program managers informed of IM/IT activities and availability and review the linkage between IM/IT activities, and HC and PHAC strategic objectives.

Recommendation

52. The Agency should implement an Information Management and Information Technology committee with proper authority and accountability to make final decisions on matters specific to Information Management and Information Technology across the Agency, subject to Executive Committee approval as appropriate.

Alignment of IM/IT Services with the Agency's Strategic Plan

Sub-Criterion: The IM/IT Strategic Plan is aligned with the Agency's Strategic Plan.

53. The Public Health Agency of Canada - Strategic Plan: 2007-08 – 2012-13, Information, Knowledge, and Action set out the Agency's key strategic objectives. PHAC has identified three strategic objectives, and a set of action areas stemming from each, to guide its actions over the next five years :

- Anticipate and respond to the health needs of Canadians;
- Ensure actions are supported by integrated information and knowledge functions; and
- Further develop PHAC's dedicated, professional workforce by providing IT with the tools and leadership it needs and by ensuring a supportive culture.

54. The IM/IT Strategic Plan had the following priorities:

- Provide IM leadership;
- Align IM/IT investments with key Agency priorities; and
- Establish Agency wide IM/IT governance.

55. The IM/IT priorities were determined based on the Directorate's knowledge of PHAC's specific context: the recognition of the recent creation of the Agency; the former culture where Programs exercised autonomy with

regard to IM/IT operations; and a definite need to structure and formalize the IM/IT decision process.

56. Some of IM/IT Directorate's accomplishments in recent months include:

- An Agency-wide IM/IT governance model was developed and piloted;
- IT Security capacity was increased to ensure the safeguarding of corporate assets;
- IM/IT infrastructure and services were consolidated. Infrastructure supporting Science and Research included: storage area Network, common server platform, increased bandwidth, etc;
- Capacity for centralized IM services was enhanced and IM measures such as the deployment of hardware infrastructure were implemented; and
- CIO consultations with PHAC management on the Agency Wide IM/IT governance were initiated.

57. The TB Guide on Strategic Planning - Tips and Advice for IM or IT Strategic Plans suggests the following checklist in developing strategic objectives:

- Objectives should clearly state the specific results that the organization seeks to accomplish in achieving its goals;
- Each goal should have at least one objective; however, an organization often has multiple objectives under a single goal;
- Measures for each objective are expressed in a quantifiable form and indicate the degree to which an organization is achieving its objectives, in view of a goal;
- Measures are directly related to the objective it is measuring. There should be at least one measure for each objective; and
- Measures indicate the change or differences that demonstrate progress (or the lack thereof) against strategic objectives. Strategic objectives and measures should be clear and easily understood by those who are unfamiliar with the organization.

58. We noted that, although programs have managed the Surveillance activities, these activities were not specifically included in the IM/IT Strategic Plan. We believe that the absence of references to major program operations, such as Surveillance activities, and the absence of specific quantitative measures directly related to the objectives they are measuring could result in inadequacies to sustain the Agency strategies and objectives.

Recommendation

59. The Chief Information Officer should ensure that the next Information Management and Information Technology Strategic Plan is aligned with the Agency's Strategic Plan and includes appropriate performance objectives.

Governance Framework

Sub-Criterion: A formal governance framework guides the IM/IT strategies and activities.

60. In order to maximize the IM/IT strategic planning exercise, CobiT suggests that the planning process be embedded into an IM/IT policy that defines when and how to perform IT strategic planning, document the approach to be followed and publicise the process to all staff.

61. CobiT also suggests that the strategic planning exercise, as any strategic decision or project implementation, should follow a governance framework that describes the IM/IT governance processes, roles, and responsibilities. The framework establishes and documents the governance and management protocols and standards to be followed for approving and implementing any IM/IT strategies and initiatives.

62. The Office of the CIO has not yet established a formal process (governance framework) for the development of its Strategic Plan. However, the IM/IT governance model recently developed as noted earlier in the report could form the basis of the development of a formal governance framework. Once developed, the implementation of a formal governance framework would result in coordinated efforts, greater transparency, effective risk management, timely communications, effective use of resources, and professional accountability.

Recommendation

63. The Information Management and Information Technology Directorate should formalize and document the Information Management and Information Technology strategic planning exercise.

Policy Framework Implementation and Conformance Measurement Processes

Sub-Criterion: The IM/IT policy framework is updated and the level of policy implementation monitored.

64. The IM/IT policies are required since they set the tone as guide and control of information systems and related resources. It is important that they are developed in a collaborative process and communicated well to staff.

65. The IM/IT policy framework includes TB policies, HC and PHAC policies, standards, and practices. The framework is comprehensive and covers the main aspects of information technology requirements. Some of these policies and the organizations they belong to are listed on the following page:

- Treasury Board:
    - Guide on Strategic Planning (2008-07-17);
    - Policy on Management of IT (2007-06-26);
    - Policy Framework for Information and Technology (2007-06-26);
    - Technology Management Strategies (2005-06-13); and
    - TB Information and Technology Standards (2003-12-15).
- Health Canada:
    - Roles and Responsibilities (2008-06-12);
    - Interim Directive on the Procurement and Management of Software (2008-04-07);
    - Interim Directive on the Procurement and Management of IT Hardware (2008-01-03);
    - Interim Directive on the Use of Personal Printers (2008-01-03);
    - Re-Use, Disposal and Destruction of IT Media (2007-07-23);
    - IT Security Policies: IT Security Policy and Guidelines and Standards - Use of Electronic Networks (2006-02-03); and
    - PPHB - Policy on LAN/PC Services (2001-11-7).
- Public Health Agency of Canada:
    - IT Security, Password Standard (2007-08-01);
    - IM/IT Security - Risk Management (2007-05-11);
    - Acceptable Use of Electronic Networks (2006-11-17);
    - PHAC IT Security Policy (2006-07-19);
    - Policy on Desktop Usage, National Capital Region (2005-03-31); and
    - Wireless Device User Agreement

66. We noted that the HC policies listed above have not yet been reviewed and updated to reflect the Agency's new environment, and evolving technology. Policies stipulating IT security requirements, roles and responsibilities, procurement, management of IT application, and hardware, in particular, need to be updated on a priority basis and tailored to PHAC's specific circumstances.

67. Policies tailored to the specific business needs of the Agency will strengthen the IM/IT Directorate's responsibility and accountability across the Agency. PHAC specific policies will formalize the compliance monitoring role of the IM/IT Directorate.

Recommendations

68. The Chief Information Officer should review and adapt existing Health Canada Information Management and Information Technology policies

currently being used by the Agency to reflect the Agency's new environment, and evolving technology.

69. The Chief Information Officer should monitor and periodically report on the Agency compliance with key Information Management and Information Technology policies.

Exercise of Leadership

Sub-Criterion: The Office of the CIO takes effective steps to ensure that PHAC IT assets, practices, investments and policy requirements are managed effectively and consistently across the Agency.

70. The Office of the CIO has been mandated to take a leadership role in IM/IT directly linked to the achievement of PHAC's strategic objectives.

71. The objectives associated with these strategic objectives are to define, build and maintain an information infrastructure that promotes good information management, system development, and system maintenance practices throughout PHAC. To attain these objectives, an integrated IM and IT environment is required for all areas of PHAC.

72. The Office of the CIO does not directly manage all IT services. Preliminary interviews disclosed that scientific projects/activities with IT components are managed without the involvement of the Office of the CIO. However, we were unable to readily identify additional significant IT expenditures that would have been reported in the financial statements as expenditures other than IT.

73. Traditionally IM/IT activities took place within the individual programs and IM/IT staff reported only to their respective programs. In addition, some programs have put in place their infrastructure, acquired the technologies, assets, and support from vendors, and contractors that they needed to accomplish their work.

74. The existence of "islands of IT" outside the purview of the IM/IT Directorate can be sub-optimal and exposes PHAC to undue risk that systems may be developed or administered without appropriate risk management and control or attention to the effective use of scarce resources. Further, it impedes the ability of the IM/IT Directorate to ensure that all IT resources are being used to support the Agency's strategic objectives.

75. When the Agency implements our recommendation calling for the establishment of an IM/IT committee, the structure will then be in place to address the leadership issues noted above.

Relations with the Service Provider: Health Canada

Sub-Criterion: Service level management process is formalized in the MOU between PHAC and HC.

76. PHAC shares common infrastructure with HC. The MOU between HC and PHAC contains the following:

- HC's authority over PHAC's IM/IT infrastructure;
- The functional authority exercised by HC's CIO over the IM/IT common services, infrastructure, and standards as long as PHAC operates within HC technical infrastructure;
- The leadership maintained by the CIO of HC over the Computer Science Community at PHAC;
- The PHAC compliance with specific HC IM/IT policies, standards, and practices for services rendered by HC;
- The level of service provided to the PHAC based on the level of service previously provided to the PPHB of HC; and
- The need for metrics to define and measure and report on services performance and services rendered by HC as per the Service Level Agreement.

77. We noted that HC and the IM/IT Directorate are operationally interdependent. However, there appears to be a tendency on the part of HC's Information Management Services Directorate (IMSD) to continue to view PHAC in the light of its former relationship to HC. Consequently, HC expects that the Agency will conform to HC IM/IT standards, policies and practices whether or not these are appropriate for PHAC.

78. We noted that a Shared Services Management Committee exists to monitor the operations as a result of the MOU. However, to modify the MOU, we believe the Office of the CIO will need the EC's direction and support in its negotiations with HC on strategic issues that the Agency may want to adopt in the future.

79. Additional requirements related to security are discussed in the section entitled -Information Security Governance.

Recommendation

80. The Agency should renegotiate the provisions of the Memorandum of Understanding with Health Canada that relate to Information Management and Information Technology in order to include service standards for infrastructure, staff and performance measurement.

IM/IT Resource Management

Criterion: The IM/IT activities are adequately structured and funded.

81. Resource management is about establishing and deploying the right IT capabilities for business needs. It primarily targets human resources, including knowledge, skills, and infrastructure. It enables an organization to leverage knowledge and skills internally and externally. It recognizes the importance of people, and, therefore, focuses on maintaining availability, providing training, promoting retention, and ensuring competent IT personnel.

82. Resource management also ensures that an integrated, economical IT infrastructure is provided; new technology, hardware and software are introduced as required by the organization; and obsolete systems are updated or replaced.

83. Resource management includes dealing with such issues as outsourcing, and trusted suppliers.

Organizational Structure and Staffing

84. The Office of the CIO is an essential part of the operations of the Agency. It is the steward of a complex environment that has continuously evolved in the past five years to provide a large and comprehensive inventory of systems and applications to the Agency.

85. The Office of the CIO provides support to all Agency personnel on messaging, telecommunications, local and wide area networks, applications, and distributed computing components related to desktops and servers.

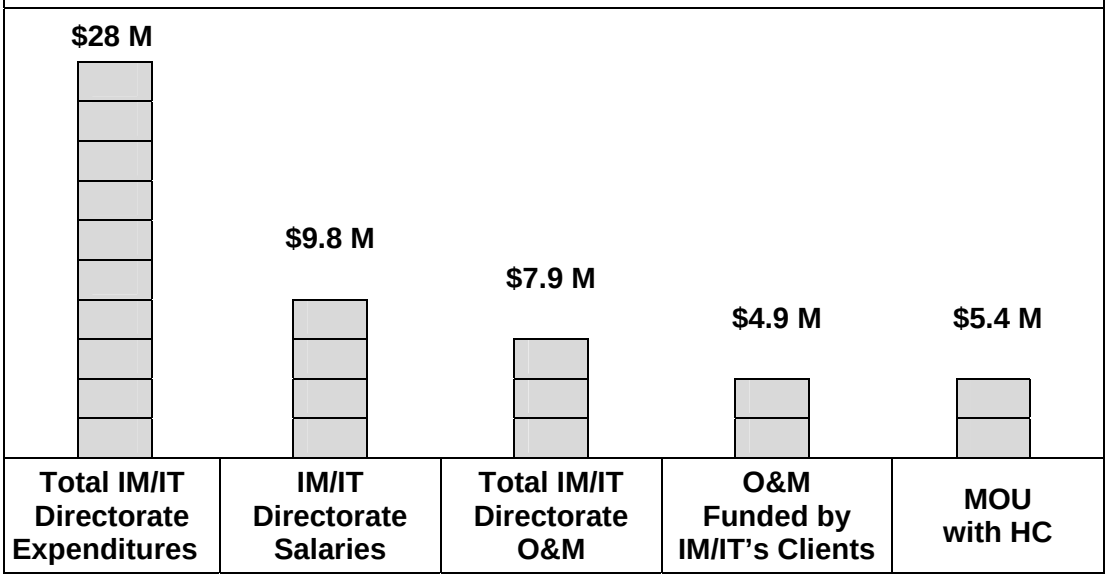
86. We could not determine if the IM/IT function is adequately staffed without conducting an in-depth review of human resources. However, we observed numerous transfers of IT staff from HC to the Agency at all levels, which indicates that the PHAC can attract new employees. In addition, interviews revealed that the Office of the CIO recognizes the importance of people, provides required training, and ensures competent employees.

Funding

87. The IM/IT Directorate has reported to the Office of the CFO that it does not have a budget sufficient to support the services and infrastructure that it is expected to manage for its clients within PHAC and faces shortfalls in O&M allocations. Table 1 presents the IM/IT expenditures in salaries and O&M. Total IM/IT expenditures amounted to $22.6 million. Salaries represented $9.8 million and O&M represented $12.8 million. Of this amount, $4.9

million was funded by IM/IT Directorate clients. An additional $5.4 million was for the MOU with HC.

Table 1: IM/IT Directorate Expenditures, FY 2007-08

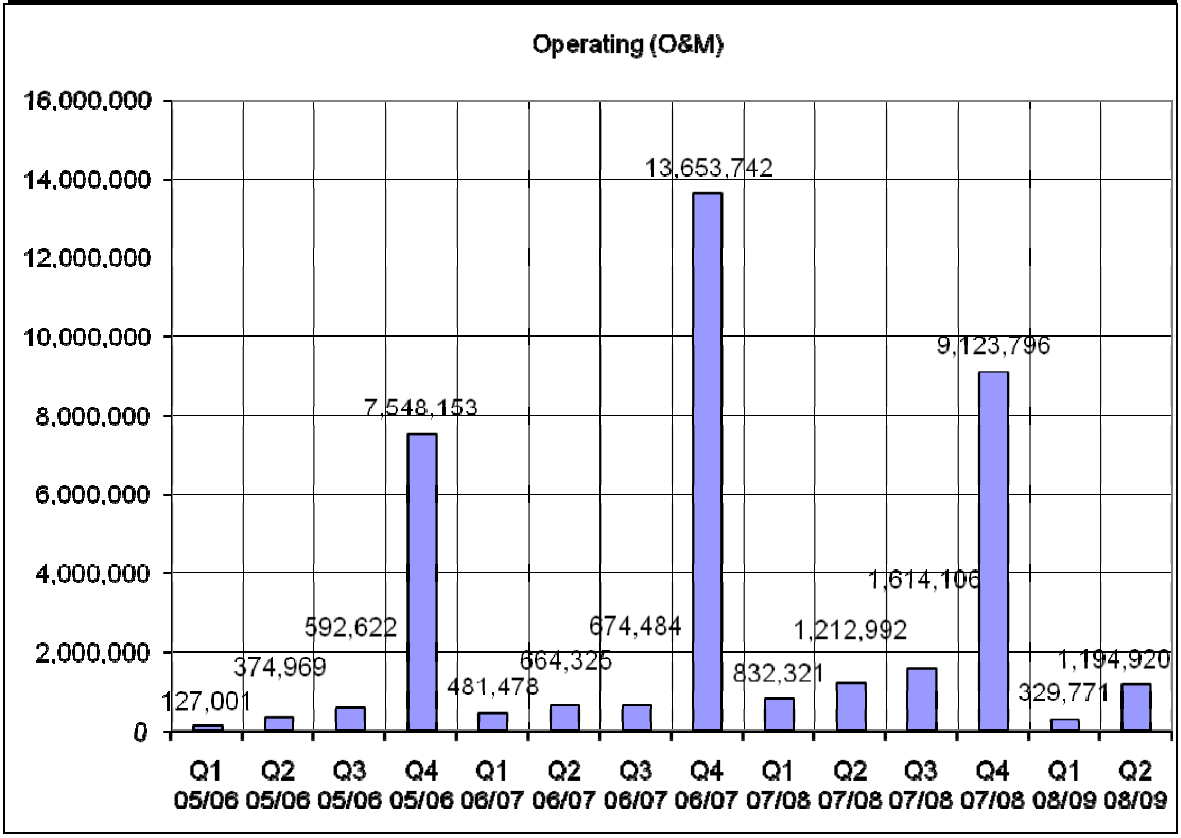


88. The initial O&M allocation for IM/IT in FY 2007-08 was $5.995 million, which is less than half the amount required by IM/IT. Of approximately $12.8 million of O&M spending by IM/IT in FY 2007-08, over $8.5 million (68 per cent) occurred in Q4 (January to March) and nearly $7 million occurred in March (Table 2: Year-end Spending). This $7 million was funded from lapsing departmental funds. This pattern has been happening since the creation of PHAC in FY 2004-05 as shown in Table 3.

Table 2: Year-end Spending (Selected Items) FY 2007-08

	Last 3 Months	Year Total	%
Computers & parts (screens & printers)	$3,718,131	$5,248,957	71 %
Computer software	$3,080,658	$3,627,341	85 %
Information technology consultants	$1,372,192	$2,483,402	55 %
Small desktop, personal portable	$418,229	$1,320,215	32 %
Total	$8,589,210	$12,679,915	68 %

Table 3: O&M Expenditures by Quarters from April 2005 to August 2009



89. The IM/IT Directorate reported that since the Agency was created, it has obtained year-end funding for infrastructure purchases, but has not been funded for the corresponding implementation and ongoing sustainment activities that should accompany these purchases. As a result, the IM/IT Directorate has taken on obligations (e.g.: maintenance and licensing) that have not been funded on an ongoing basis.

90. The IM/IT Directorate has routinely submitted business cases to the Office of the CFO to make up for funding shortfalls. Unfortunately, the funding obtained was often one time funding, so the IM/IT Directorate was obliged to regularly resubmit similar business cases in order to obtain the funding required to sustain previous investments.

91. Best practices suggest that IM/IT be funded between 4.3 and 4.7 percent of the organization's total budget. The IM/IT Directorate currently manages $12.8 million in direct funding and $5.4 million through the MOU with HC for a total of $18.2 million. This represents just 3.0 percent of PHAC's overall budget ($590.5 million for FY 2008-09). To reach the range suggested by the industry, IM/IT funding should be between $25.4 and $27.8 million.

92. In order to resolve the situation, the IM/IT Directorate suggested a reallocation process to divert funding from programs to IM/IT in order to alleviate the problems described above.

93. The Agency does not have an approved multi-year budget allocation for IM/IT. Without such budgets, the IM/IT Directorate cannot adequately plan for the three-year hardware replacement, an industry best practice. Instead, purchases are made in bulk at year-end without consideration of PHAC priorities. The goal of reducing the year-end lapse seems to override the need for effective planning in the allocation of IT resources.

94. A further consequence of not having an approved multi-year budget is limiting the organization's ability to provide integrated, economical IT infrastructure, to introduce new technology, replace obsolete systems and get involved in the user-requested application development.

Recommendations

95. The Chief Financial Officer and the Chief Information Officer should review the level of Information Management and Information Technology funding in accordance with best practices.

96. The Agency should implement a multi-year budget allocation for Information Management and Information Technology.

Acquisition of Automated Solutions

Criterion: Processes are in place to identify, acquire, test and monitor automated solutions.

97. The acquisition of automated solutions involves the procurement of hardware, software, and services to effectively support programs. Ideally, IT acquisitions would be fully integrated within the Agency and follow the IM/IT Directorate's standards for the acquisition of IT resources.

98. Automated applications need to be designed, developed, configured, and implemented in line with an appropriate system development life cycle methodology and installed as per program requirements. They must also include proper application controls, and security requirements.

99. The performance measurement domain closes the loop and provides feedback on existing and newly acquired automated solutions by providing evidence that procurement initiatives are on track and create value for PHAC.

Acquisition of Hardware

100. As noted in the previous section under Funding, the PHAC IM/IT funding and expenditure trends showed that acquisition of hardware occurs at year-end and depend mainly on programs' year-end surplus instead of an IM/IT priority and strategic direction.

Software

101. PHAC and HC share major corporate applications such as SAP (Systems Applications Products, the central financial system), HR Advantage (an application managed by the HC HR Directorate), ILAM (Interactive Leave and Attendance Module, an application managed by the HC HR Directorate), etc. PHAC has also implemented its own corporate applications, such as an Application Inventory Registry.

102. PHAC's data processed by HC corporate applications are intermixed with that of HC to the extent that, in some instances, HC would experience difficulties to segregate PHAC data from its own data. These corporate applications were developed and financed by programs when PHAC was still a Branch of HC.

103. The IM/IT Directorate has identified several applications to be developed in the next few years but funding is not fully available. The large demand for new software and the lack of funds have resulted in numerous application developments being indefinitely postponed. In such circumstances, clients opt for alternative solutions such as third party developers or the acquisition of "off the shelf" software. These solutions are not optimal since "off the shelf" software often requires extensive customization at the time of implementation. The IM/IT Directorate is called upon to provide additional support in these circumstances.

Recommendation

104. The Chief Information Officer should approve all Information Management and Information Technology acquisitions of hardware and software based on Agency identified priorities and strategic direction.

Performance Measurement

Sub-Criterion: There exists a performance measurement system linking IT performance to PHAC goals.

105. Performance measurement can help ensure that an integrated and economical IT infrastructure is provided, and that appropriate service levels are met.

106. The IM/IT Directorate has requested from HC, without success, sets of metrics that would provide insight into the outcomes and performance of the processes managed by HC. These metrics would help reduce risks and improve efficiency. They would also help reduce errors and allow for a more consistent management approach. The metrics should be included in the MOU renegotiations suggested earlier.

107. Without establishing and monitoring performance measures, it is unlikely that IT strategic alignment, IT resource management, and IT risk management will be adequately informed on the achievement of results.

Recommendation

108. The Agency should negotiate an enhanced commitment from Health Canada to support the Agency's performance measurement needs.

Information Security Governance

Criterion: Risks are adequately assessed and managed.

109. Information security governance is a component of IT governance, with the specific value drivers of information integrity, service continuity (availability), and information asset protection (confidentiality).

110. Dependence on information and IT systems has grown in the last two decades. Accordingly, information security has become an important and integral part of IT governance, and information security governance has become increasingly critical. Leadership, organizational structures, and processes are required to safeguard electronic information.

111. Information security governance is the responsibility of the CPHO since it has a direct relationship to the governance element "Risk Mitigation". In PHAC, the CIO, the Departmental Security Officer (DSO) and senior management are involved in the management of the Information security.

Threat and Risk Assessments and Statement of Sensitivity for New Applications

Sub-Criterion: The level of protection and handling of the information assets are adequately defined.

112. Interviews disclosed that program staff often forget to complete Threat and Risk Assessments (TRA) and Statement of Sensitivity (SoS) of information when developing applications and storing information on private networks. Nevertheless, the situation appears to have improved in the past year and the IM/IT Directorate has received many SoS from Program staff lately.

113. The lack of TRA and SoS is partly due to the fact that IM/IT Directorate does not have control over all applications development projects. Presently, program managers have the authority and accountability to identify the sensitivity, privacy, availability, and integrity levels of information assets. The decentralization of these decisions creates an undue risk that PHAC's desired security profile may be compromised.

Network Services

Sub-Criterion: PHAC shared applications are accessed over the Health Portfolio LAN/WAN architecture and meet risk requirements.

114. PHAC network perimeter services include numerous players: HC, PWGSC (under contract with HC), PHAC and third parties. Changes made to the shared Health Portfolio network perimeter services could affect PHAC infrastructure and network security.

115. PHAC has a low tolerance for risk while HC and PWGSC have a medium tolerance. The majority of the Health Portfolio systems do not require such a high level of security, but a number of PHAC surveillance and critical information systems contain sensitive data, which requires extra security safeguards. Normally, the level of protection required for data that are stored or transmitted across a network dictates the security level that the organisation should put in place. The current networking environment exposes PHAC to greater risks due to the difference in acceptable risk tolerance levels between the HC network environment and certain PHAC network environments.

116. Due to the current HC network risk assessment, PHAC programs are sometimes not allowed access to external data holdings. There is a need for PHAC sensitive systems and their associated data to be stored on a more secure network, since they cannot reside on the HC medium-risk tolerant network, unless additional security safeguards are implemented.

Changes to the Health Portfolio LAN-WAN environment

Sub-Criterion: Changes to the Health Portfolio LAN/WAN architecture are approved only after a comprehensive assessment of their impact is completed and PHAC is consulted.

117. The IM/IT Directorate has noticed a few improvements in the responsiveness and support for PHAC initiatives and changes received from Health Canada's IMSD over the past few months. Examples of such improvements include:

- Improved communications between PHAC and HC on IT challenges, initiatives, and changes through a higher representation of PHAC IT management at the weekly HC IT operations meetings;
- Quicker response time from HC on addressing problems with the Norton Antivirus; and
- Improved process when clients require a change in the Web filters.

118. Implementation of new PHAC applications and systems may incur greater risk as they reside within the HC (PWGSC) medium security risk level.

119. Any new applications and systems hosted on the HC-Net must undergo the HC Change Management approval process. This change management process is appropriate and PHAC is in the process of implementing a similar process for those systems it hosts independently of HC.

Recommendations

120. The Agency should implement an internal Information Technology change management process, with appropriate authorities.

121. The Agency's responsible officer for change management should ensure that appropriate Information Management and Information Technology security risks are reviewed and addressed through statements of sensitivity and threat and risk assessments for existing and new applications that are developed and hosted on local and wide area networks used by the Agency.

122. Periodic reviews of the risk tolerance levels should be jointly undertaken by the Public Health Agency of Canada and Health Canada in order to provide the most suitable Information Technology security baseline for shared services.

Acquisition, Safeguard and Disposal of Electronic Data

Criterion: Processes are in place to acquire, retain, archive, and dispose of electronic data.

123. Effective data management requires the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of electronic information. Responsibility for data ownership and management should be clearly defined, assigned and communicated within the organisation. Procedures need to be formalized and widely known. Formal training for data management staff members should be in place.

Legislated IM Requirements

Sub-Criterion: There is an IM awareness program to inform employees of the importance of IM practices, their responsibilities, and potential areas for improvement.

124. Where IM services are available in PHAC, they are not necessarily aligned with Government of Canada standards and do not meet policy requirements in terms of identification, classification, retention and disposal. Employees and management across the Agency do not always understand policy requirements or the importance of good information management practices.

Consequently, information is not safeguarded, managed, and disposed of effectively or efficiently.

125. The IM management recognizes the necessity to implement an IM awareness program for personnel in order to inform them of the importance of IM practices, their responsibilities, and potential areas for improvement. An effective awareness program enhances chances that information is adequately safeguarded, managed, and disposed effectively or efficiently. Clear and robust information management systems and practices will also be of assistance to the Agency for retrieval and organization of materials for any subsequent proceedings. .

CIO Authority with Regard to the Acquisition, Safeguard, and Disposal of Electronic Data

Sub-Criterion: Processes for the acquisition, safeguard, and disposal of electronic data are properly managed**.**

126. The CIO does not currently have the required authority and resources to enforce standards or to measure enforcement and/or compliance with TB and PHAC requirements for acquisition, safeguard, and disposal of electronic data.

127. PHAC has a significant amount of electronic information assets but has limited control over their management. The volume of information has been increasing year over year while the resources dedicated to its management have not kept pace.

Corporate Electronic Information Management Program

Sub-Criterion: There exists a centralized and funded corporate Information Management Program.

128. A centralized and funded corporate IM program is lacking thus there is limited corporate oversight of electronic information management activities.

129. Interviews revealed that PHAC has not taken advantage of a centralized recruitment process. Programs hire their own information management functionalists, typically term employees who do not have the opportunity to acquire the skills and competencies to perform their functions. The constant turn-over among these term employees jeopardizes the integrity of the records management system and the inventory of information holdings.

Information Holdings

Sub-Criterion: The inventory of electronic information holdings is complete and up-to-date.

130. A significant portion of the Agency's electronic records are not captured. As a result, such electronic records cannot be categorized and managed according to an established lifecycle management. Consequently, this information is unmanaged, uncategorized, not easily accessible and verifiable, and its lifecycle is not determined.

131. In order to improve the above condition, the IM/IT Directorate has undertaken numerous activities:

- Piloted the implementation of Records, Document and Information Management System, a suite of software applications designed to provide an economical software solution for records and document management;
- Provided user education and awareness;
- Developed and implemented a PHAC classification structure;
- Drafted multi-year retention schedule; and
- Drafted PHAC IM policy and records procedures manual.

132. The absence of a definitive electronic records solution results in e-records being stored in many locations including: shared drives, lotus notes e-mails and databases. Some information could be lost on an employee's departure when it has not been inventoried.

Recommendation

133. The Agency should enforce Government of Canada standards related to electronic data, including the creation of a centralized and funded corporate Information Management Program, the completion of an inventory of electronic information holdings, and the implementation of an electronic information awareness program within the Public Health Agency of Canada.

Conclusion

134. Established less than four years ago, PHAC has made some progress in building its IM/IT governance. The EC provided strategic orientations and direction to the Office of the CIO. However, there are several key areas where improvements need to be made. The improvements will enable IT to support the PHAC's strategic objectives and will ensure that IM/IT systems and processes effectively support the management and professional information needs of PHAC in a well controlled environment.

135. While most of the recommendations in this report are directed at the CIO, implementing the recommendations will require the full support of the Executive Committee.

Acknowledgments

136. We wish to express our appreciation for the cooperation and assistance afforded to the audit team by management and staff during the course of this audit.

Appendix A – Audit Criteria

1. IM/IT Management Framework

Criterion

An IM/IT management framework exists for decision, direction, and accountability. This framework is well understood and accepted by PHAC managers.

Sub-Criteria

a. Senior Management provides IM/IT with direction and support on horizontal issues that relate to network architecture improvement, application development, and investment decisions that IM/IT could incorporate into its Strategic Plan.

b. The Office of the CIO is informed of major IM/IT plans of the Programs and has the authority and resources to ensure that such plans are implemented in accordance with PHAC's IT governance policies.

c. The IM/IT Strategic Plan is aligned with the Agency's Strategic Plan.

d. A formal governance framework guides the IM/IT strategies and activities.

e. The IM/IT policy framework is updated and the level of policy implementation monitored.

f. The Office of the CIO takes effective steps to ensure that PHAC IT assets, practices, investments and policy requirements are managed effectively and consistently across the Agency.

g. Service level management process is formalized in the MOU between PHAC and HC.

2. IM/IT Resource Management

Criterion

The IM/IT activities are adequately structured and funded.

3. Acquisition of Automated Solutions

Criterion

Processes are in place to identify, acquire, test and monitor automated solutions.

Sub-Criterion

There exists a performance measurement system linking IT performance to PHAC goals.

4. Information Security Governance

Criterion

Risk are adequately assessed and managed.

Sub-Criteria

a. The level of protection and handling of the information assets are adequately defined.

b. PHAC shared applications are accessed over the Health Portfolio LAN/WAN architecture and meet risk requirements.

c. Changes to the Health Portfolio LAN/WAN architecture are approved only after a comprehensive assessment of their impact is completed and PHAC is consulted.

5. Acquisition, Safeguard, and Disposal of Electronic Data

Criterion

Processes are in place to acquire, retain, archive, and dispose of electronic data.

Sub-Criteria

a. There is an IM awareness program to inform employees of the importance of IM practices, their responsibilities, and potential areas for improvement.

b. Processes for the acquisition, safeguard, and disposal of electronic data are properly managed.

c. There exists a centralized and funded corporate Information Management Program.

d. The Inventory of electronic information holdings is complete and up-to-date.

Appendix B – Management Action Plan

Recommendation	Management Response	Officer of Prime Interest	Target Date
IM/IT Management Framework			
47. The Executive Committee should obtain regular updates on Information Technology management from the Chief Information Officer.	Agree. The Chief Information Officer (CIO) will provide regular updates to the Executive Committee (EC).	CIO	March 31, 2009
52. The Agency should implement an Information Management and Information Technology committee with proper authority and accountability to make final decisions on matters specific to Information Management and Information Technology across the Agency, subject to Executive Committee approval as appropriate.	Agree. An Information Management and Information Technology (IM/IT) committee will be formed, reporting to the EC. This committee is chaired by the Senior Assistant Deputy Minister (SADM) and vice-chaired by the CIO.	SADM	December 2008
59. The Chief Information Officer should ensure that the next Information Management and Information Technology Strategic Plan is aligned with the Agency's Strategic Plan and includes appropriate performance objectives.	Agree. The next IM/IT Strategic Plan will address program priorities identified through the IM/IT Governance committee and will address top level priorities identified in the Agency's Strategic Plan.	CIO	September 30, 2009
63. The Information Management and Information Technology Directorate should formalize and document the Information Management and	Agree. The IM/IT Directorate will adopt a planning cycle for the update and refresh of the IM/IT Strategic Plan, including linkages	CIO	March 31, 2009

Information Technology strategic planning exercise.	to the appropriate governance bodies and the corporate and functional planning cycles.		
68. The Chief Information Officer should review and adapt existing Health Canada Information Management and Information Technology policies currently being used by the Agency to reflect the Agency's new environment, and evolving technology.	Agree. The IM/IT Directorate will undertake a systematic and prioritized review and refresh of policies. Prioritizing and approving PHAC policies will be referred to the PHAC IM/IT Management committee.	CIO	Started in April 2008 and will be fully implemented by March 2010
69. The Chief Information Officer should monitor and periodically report on the Agency compliance with key Information Management and Information Technology policies.	Agree. The IM/IT Directorate will monitor and report on the Agency IM/IT policy compliance through the Agency's governance and reporting structures.	CIO	April 2010
80. The Agency should renegotiate the provisions of the Memorandum of Understanding with Health Canada that relate to Information Management and Information Technology in order to include service standards for infrastructure, staff and performance measurement.	Agree. The SADM and the CIO will continue to participate in the shared services management committee and will continue to actively manage the services provided by Health Canada (HC) to obtain the best possible outcome for the Agency.	SADM and CIO	March 2009
IM/IT Resource Management			
95. The Chief Financial Officer and the Chief Information Officer should review the level of Information Management and Information Technology funding in accordance with best practices.	Agree. The Chief Financial Officer (CFO) will review priorities in view of reallocated resources.	CFO	March 2009

96. The Agency should implement a multi-year budget allocation for Information Management and Information Technology.	Agree. The CFO will implement a multi-year budget allocation for IM/IT.	CFO	March 2010
Acquisition of Automated Solutions			
104. The Chief Information Officer should approve all Information Management and Information Technology acquisitions of hardware and software based on Agency identified priorities and strategic direction.	Agree. The acquisition and development of automated solutions will be discussed and prioritized at the IM/IT Governance committee. Funding for these activities will be discussed at the appropriate governance committees.	CIO	April 2009
108. The Agency should negotiate an enhanced commitment from Health Canada to support the Agency's performance measurement needs.	Agree. The CIO will continue to advocate for better management of the services provided under the Memorandum of Understanding with Health Canada; in particular, the CIO will continue to push for performance management metrics for IM/IT services.	SADM and CIO	March 2009
Information Security Governance			
120. The Agency should implement an internal Information Technology change management process, with appropriate authorities.	Agree. The IM/IT Directorate will implement a PHAC IM/IT change management process.	CIO	April 1, 2009
121. The Agency's responsible officer for change management should ensure that appropriate Information Management and Information Technology security risks are reviewed and addressed through	Agree. The PHAC IM/IT change management process will include linkages to IT security and risk management processes.	CIO	April 1, 2009

statements of sensitivity and threat and risk assessments for existing and new applications that are developed and hosted on local and wide area networks used by the Agency.	Additionally, the IM/IT Directorate will work with PHAC programs to complete security documentation for existing critical IM/IT systems.	CIO	December 2010
122. Periodic reviews of the risk tolerance levels should be jointly undertaken by the Public Health Agency of Canada and Health Canada in order to provide the most suitable Information Technology security baseline for shared services.	The CIO will continue to advise PHAC senior management on the risks associated with IM/IT infrastructure and services and work with service providers (including HC and Public Works and Government Services Canada) to mitigate and manage risk. The assessment of the PHAC risk tolerance level will be a periodic agenda item for the PHAC IM/IT Governance committee.	CIO	March 2010
Acquisition, Safeguard, and Disposal of Electronic Data			
133. The Agency should enforce Government of Canada standards related to electronic data, including the creation of a centralized and funded corporate Information Management Program, the completion of an inventory of electronic information holdings, and the implementation of an electronic information awareness program within the Public Health Agency of Canada.	The CIO will continue to work towards compliance with Government of Canada standards through the Records, Document and Information Management System pilot project, staff training and awareness and policy development for the management of electronic records	CIO	December 2011

Appendix C – List of Acronyms

ADM	Assistant Deputy Minister
Agency	Public Health Agency of Canada
ASD	Audit Service Division
CCDPC	Center for Chronic Disease Prevention and Control
CFO	Chief Financial Officer
CIO	Chief Information Officer
CobiT®	Control Objectives for Information and Related Technology
CPHO	Chief Public Health Officer
DSO	Departmental Security Officer
EC	Executive Committee
FY	Fiscal Year
ILAM	Interactive Leave and Attendance Module
HC	Health Canada
IDEP	Infectious Disease and Emergency Preparedness Branch
IM/IT	Information Management/Information Technology
IMSD	HC Information Management Services Directorate
LAN	Local Area Network
MOU	Memorandum of Understanding Between HC and PHAC
O&M	Operation and Maintenance
PHAC	Public Health Agency of Canada
PPHB	Public Population Health Branch
PWGSC	Public Works and Government Services Canada
SADM	Senior Assistant Deputy Minister
SAP	Systems Applications Products
SoS	Statement of Sensitivity
TB	Treasury Board
TRA	Threat and Risk Assessment
VPN	Virtual Private Network
WAN	Wide Area Network