Travaux publics et Services gouvernementaux Canada

Public Works and Government Services Canada

Canada

Respect • Intégrité • Excellence • Leadership

Au service du GOUVERNEMENT, au service des CANADIENS.

Final report

Audit of governance of Public Works and Government Services Canada's business application portfolio

March 31, 2016
Office of Audit and Evaluation

www.pwgsc-tpsgc.gc.ca

Table of contents

Executive summary i
Introduction 1
Background 4
Focus of the audit 5
Statement of conformance 5
Observations 6
Conclusion 15
Management response 16
Recommendations and Management Action Plan 16
About the audit 20

Executive summary

i. PWGSC is one of the largest federal government organizations in Canada. It provides common services to more than 100 federal departments and agencies, which deliver services to Canadians. Many of these services are information technology (IT) dependent; as such PWGSC relies heavily on IT.

ii. In 2010, the Office of the Auditor General performed an audit of aging IT systems across five federal government departments, which included PWGSC. It observed that aging IT applications and infrastructure used to deliver key services to Canadians may pose risks that could affect the security or operability of the applications and systems. It also observed that IT applications and infrastructure should be managed on a portfolio basis.

iii. In response to the recommendations made by the Office of the Auditor General, PWGSC's Office of the Chief Information Officer identified actions to address the findings related to managing aging IT applications, which included developing an IM/IT Portfolio Management Framework, enhancing its IT governance framework, developing a multi-year IM/IT investment plan, and developing a departmental IT risk profile.

iv. In addition, Treasury Board Secretariat developed an Application Portfolio Management Strategy to assist departments in managing their aging IT applications on a portfolio basis.

v. Starting in 2014, the CIO Branch, in collaboration with the other branches in PWGSC, transferred the responsibility and resources for the majority of run (maintenance) activities to the CIO Branch. This transfer resulted in over 100 employees being transferred along with funding of approximately $23M being permanently transferred, with another $11.7M that is transferred annually due to source of funding considerations (money attached to revolving funds, special allotment purposes, etc.). The Branch was also reorganized in order to better meet the new mandate and improve client services. FY 2015-16 is the first year where the CIO Branch is fully functioning with its new operating model, i.e.: with the human and financial resources in place to support the new delivery model.

vi. The financial resources allocated to investments in increased functionality to existing applications, or to the introduction of a new application, or to the IM/IT-enablement of business transformation remains within branches, as does the decision making related to these investments.

vii. Actions taken in response to the Auditor General report contribute to managing business applications using portfolio management. The Chief Information Officer Branch has partially implemented some elements that reflect the Treasury Board of Canada Secretariat Application Portfolio Management Strategy in managing its applications on a portfolio basis. However, there are number of elements which require further work. Adoption of these elements would further enhance portfolio management, IM/IT planning, and risk management.

viii. Most significantly, we found that governance committees are not discharging their mandate related to the management of PWGSC's Business Application Portfolio. We also found that information about the existing application portfolio, which is collected through the application of the lifecycle management methodology, was incomplete. Further, Aging IT Action Plans were not available and prioritization criteria for selecting investments were not approved until 2015. As a result, governance committees were not sufficiently informed to make IM/IT investment decisions related to the Business Application Portfolio, and there is no evidence that the IM/IT Plan, in relation to the Business Application Portfolio, is based on the application of best practices and highest priorities to support Departmental investment decisions related to the Business Application Portfolio. Finally, there is limited evidence that related risks to the Business Application Portfolio are being appropriately monitored.

ix. Due to weakness in the governance for managing the Business Application Portfolio, it is not clear that IM/IT investment planning and portfolio management is based on sufficient information to inform sound decision making.

Management response

Management has had the opportunity to review the report, and agrees with the conclusions and recommendations found therein. Management also developed a Management Action Plan to address these recommendations.

Recommendations and Management Action Plan

Recommendation 1: The Chief Information Officer, Chief Information Officer Branch should update and fully implement a PWGSC Portfolio Management Framework.

Management Action Plan 1: CIO Branch will review, update, and implement Application Portfolio Management (APM) in accordance with TBS framework. This will include:

> **Management Action Plan 1.1:** Realigning client delivery functions i.e. project management to Service Management and allowing Product Management team to focus on conduct of APM, release management, and continuous service delivery model and tools improvement.
>
> **Management Action Plan 1.2:** Documenting and communicating to DG and ADM level committees the required annual APM cycle including elements, accountable organizations, deliverables, and links to other activities such as departmental IM/IT investment plan, risk mitigation, and governance.
>
> **Management Action Plan 1.3:** Reviewing the TBS framework for Application Portfolio Management, mapping to current CIO Branch practices in order to

identify gaps, e.g. applications that have not yet been assessed or partially assessed.

Management Action Plan 1.4: Presenting APM findings to the DG and ADM level committees, highlighting the gaps and priorities. This will garner support to close the gaps and address the aging IT priorities highlighted through the APM exercise. For example, applications classified as "Migrate" with higher risk due to aging infrastructure should receive higher priority for remediation.

Recommendation 2: The Chief Information Officer, Chief Information Officer Branch should enhance the governance structure that supports IT investment.

Management Action Plan 2: CIO Branch will ensure the departmental IM/IT governance committees are leveraged and are core to the revised IM/IT Investment Planning and Portfolio Management Framework and related processes. This will entail re-launching the IM/IT Governance by:

Management Action Plan 2.1: Establishing an annual schedule of meetings for both the ADM and DG level committees.

Management Action Plan 2.2: Ensuring the ADM and DG level committee understand their role by reviewing/revising the terms of reference for both the ADM and DG-level committees to ensure that the committees are supporting the new branch operating model.

Management Action Plan 2.3: Engaging the ADM and DG level committees in reviewing the Department's IM/IT Investment Plan prior to DM-level Investment Management Board decisions.

Management Action Plan 2.4: Providing a bi-annual report on change and transform activities and investments, in support of departmental IM/IT prioritization.

Recommendation 3: The Chief Information Officer, Chief Information Officer Branch should provide relevant information, such as Sustainment and Renewal Strategies, Application Roadmaps, and Aging IT Action Plans for mission critical applications, to support decision making related to investment planning and management decisions.

Management Action Plan 3: CIO Branch will document and communicate outcomes from the on-going APM analysis including results of the TIME (Tolerate, Innovate, Migrate and Eliminate) to support decision making related to Application Roadmaps, investments planning, and risk management and mitigation strategies. This will include:

Management Action Plan 3.1: Identifying, documenting and communicating mission critical and essential applications.

Management Action Plan 3.2: Documenting and communicating current TIME results as input to the annual IM/IT Investment Plan including governance, risk management, and mitigation. For example, applications classified as "Migrate" with higher risk due to aging infrastructure should receive higher priority for remediation.

Management Action Plan 3.3: Documenting and communicating planned individual branches' investment in "Change" portfolio in support of priority setting (as per actions of Recommendation 2 above).

Management Action Plan 3.4: Provide the Partner's Application Portfolio in Partner Service Agreements.

Management Action Plan 3.5: Provide quarterly updates on actual costs by application in the Partner Service Agreements.

Recommendation 4: The Chief Information Officer, Chief Information Officer Branch should strengthen the risk management processes related to legacy business applications.

Management Action Plan 4: CIO Branch will leverage the outcome from the TIME analysis to document, publish, and communicate required investment and activities related to legacy business applications in support of governance and decision making. This will include:

Management Action Plan 4.1: Documenting and communicating outcomes from the TIME analysis.

Management Action Plan 4.2: Leveraging the governance in Recommendation 2 to secure required direction and decision to support proposed risk management and mitigation strategies.

Introduction

1. This engagement was included in the Public Works and Government Services Canada (PWGSC) 2013-2018 Risk-Based Audit and Evaluation Plan.

2. As one of the largest federal government organizations in Canada, PWGSC provides common services to more than 100 federal departments and agencies, which in turn deliver programs to Canadians.

3. PWGSC relies heavily on information technology (IT). An IT system consists of both the business application and the infrastructure upon which the application runs. Shared Services Canada is responsible for managing the infrastructure for the Government of Canada, while departments are responsible for the business applications they use to deliver their services.

4. Some of these IT systems are aging; they consist of older business applications, which may also be supported by old infrastructure. These business applications create specific risks for the Department that must be managed. Renewal and modernization of IT systems is a significant undertaking that must be planned for and budgeted over the long term. The costs to renew and modernize IT systems are significant and can take many years to fund. Furthermore, implementation can take five years or more.

5. In 2010, the Office of the Auditor General performed an audit of aging IT systems across five federal government departments, including PWGSC. The purpose of the audit was to assess the condition of the government's aging IT applications and infrastructure used to deliver key programs and services to Canadians. The Office of the Auditor General defined aging IT systems as referring "not only to a system's age in years but also to issues that affect its sustainability over the long term, such as availability of software and hardware support and of the people with the necessary knowledge and skills to service these systems. The term also relates to a system's ability to adequately support changing business needs or emerging technologies such as 24/7 online availability."

6. The Office of the Auditor General observed that although a significant number of Government of Canada IT systems were meeting current needs, they were becoming increasingly expensive to operate and posed risks that could affect security or restrict the way the Government conducted its business. Among the most significant risks was the possibility that aging critical IT systems could simply fail and prevent the Government from delivering key services to the public.

7. Based on the findings, the Office of the Auditor General directed the following recommendations at PWGSC:

    i. **Recommendation 1.49:** PWGSC should use a department-wide portfolio management approach to ensure that they focus on current and planned IT

investments that best contribute to meeting their business objectives, with an acceptable degree of risk and at a reasonable cost.

ii. **Recommendation 1.50:** PWGSC should develop a multi-year IT investment plan that presents a balanced mix of mandatory, sustaining, and discretionary investments that they require to both sustain existing systems and to improve service delivery.

iii. **Recommendation 1.59:** PWGSC should develop an action plan for each significant aging IT risk. The plans should include specific strategies, key activities, deliverables, and timelines to manage these risks. This entity should report progress regularly to senior management.

8. At the time of the Auditor General report, PWGSC was responsible for managing both applications and infrastructure, which is why findings and recommendations were directed to IT systems (i.e. both business applications and infrastructure). However, with the creation of Shared Services Canada in 2011, the Department is no longer responsible for the infrastructure component of the IT systems. As such, our audit focused solely on PWGSC's responsibilities related to business applications.

9. In response to the recommendations made by the Office of the Auditor General, PWGSC's Office of the Chief Information Officer Branch (CIOB) identified a number of actions to address the issues identified. These included:

   i. Developing an **IM/IT portfolio management framework**;

   ii. Enhancing its **IT governance framework** to provide oversight of the portfolio management approach;

   iii. Developing a **multi-year IM/IT investment plan**, and

   iv. Developing a departmental **IT risk profile** and monitoring and reporting on the status of risks.

10. A portfolio is defined as a collection of assets held by an institution. An application portfolio can be seen as the set of IT-enabled business applications.

11. Furthermore, in response to the Auditor General report, in 2013, Treasury Board of Canada Secretariat (TBS) developed the Government of Canada Application Portfolio Management Strategy (the Treasury Board of Canada Secretariat (TBS) Strategy) along with a number of supporting documents, such as Government of Canada Application Portfolio Management - Lifecycle Management. The objective of applying this Strategy is to provide an IM/IT portfolio management framework to generate application decisions that are based on the best practices and highest priorities of the organization application portfolio, and to support the development of appropriate application management plans. It is also intended to assist departments in

reducing the number of applications and increasing application compliance to enterprise architecture standards.

12. More specifically, the Treasury Board of Canada Secretariat (TBS) Strategy supports portfolio management through consideration of the following elements and objectives, as applied to the entire portfolio of applications:

    i. **Application governance** consists of a rigorous governance structure that provides direction and oversight of IT management. Through joint membership of the IT manager and business application owner, it supports a shared accountability and decision making between these groups. It leverages application portfolio information, such as portfolio classification, aging IT assessment and application lifecycle management to drive application prioritization and risk planning, which is then combined with available investment resources to inform investment decisions.

    ii. **Application portfolio information** feeds IT investment decision making by providing information on sustainability and risks related to applications.

        a. **Portfolio classification** is a tool to classify and assign applications to portfolios based on their business outcomes, as defined by the Program Alignment Architecture (PAA), which is the Government of Canada reference model as per the *Management, Resources and Results Structures* (MRRS) policy. The grouping of investments by portfolio promotes a department-wide view, which helps management conclude on the appropriateness of the portfolio's balance and increases its ability to influence investment decisions on a portfolio-wide basis.

        b. **Aging IT assessments** are conducted on an annual basis to determine aging IT risks for mission critical applications and responses to mitigate those risks. For high risk mission critical applications, formal Aging IT Action Plans should be developed. Aging IT Action Plans should include specific strategies, deliverables, timelines, funding sources and IT investment required to support mission critical applications. Aging IT Assessments and Aging IT Action Plans help ensure risks that threaten mission critical systems are appropriately managed.

        c. **Application lifecycle management** is a formal assessment of technology and business value of each application using a lifecycle management methodology. The first step is an evaluation of the technical condition, business value and support cost of each application ('TIME assessment'), which identifies the planned management approach for each application: tolerate, innovate, migrate, or eliminate. Once the management approach has been identified, Sustainment and Renewal Strategies and Application Reduction Road Maps are developed to guide the management of each application.

iii. **Planned IT investment** reports on planned application investment over a five-year planning period and reflects discretionary and non-discretionary investment.

iv. **IT plan** is a multi-year plan that describes the overall IM/IT plan for the sustainment and renewal of the entire application portfolio. It should include the sources of funding and investment for a three-year period and should be integrated with the corporate departmental Investment Plan. It should include the Planned IT Investment Report, Sustainment and Renewal Strategies, and Application Reduction Road Maps, as well as Aging IT Action Plans for mission critical applications.

13. The figure below is a diagram of the key areas of the government-wide Government of Canada Application Portfolio Management (APM) Framework.

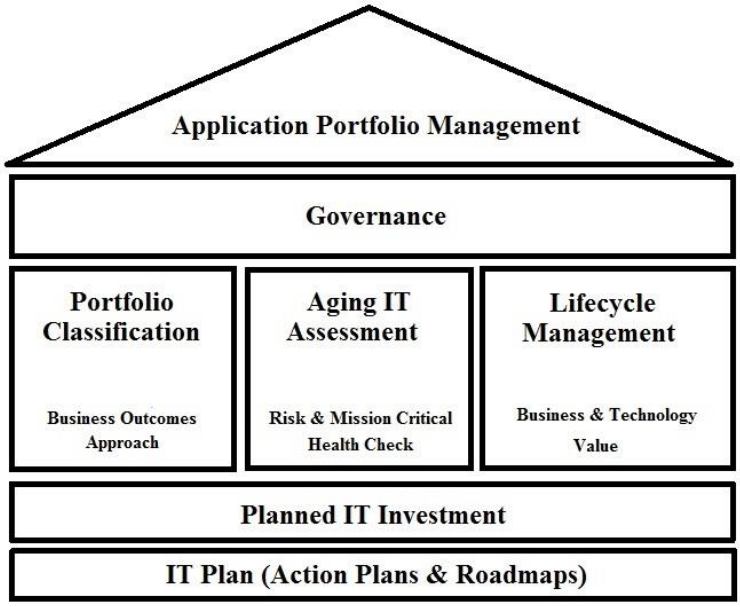

Figure 1: Application Portfolio Management (APM) Framework:
TBS - Government of Canada Application Portfolio Management Strategy

Background

14. Historically, branches within PWGSC have acted independently in maintaining and/or modernizing their applications. Because branches controlled a significant portion of the IM/IT funding, decision making was often done on the basis of branch specific requirements – resulting in duplication, isolated islands of corporate data, and significant effort to "keep the lights" on for applications where funding was not provided to ensure ongoing and regular updates to the applications.

15. Starting in 2014, the CIO Branch, in collaboration with the other branches in PWGSC, transferred the responsibility and resources for the majority of run (maintenance) activities to the CIO Branch. This transfer resulted in over 100 employees being transferred along with funding of approximately $23M being permanently transferred, with another $11.7M that is transferred annually due to source of funding considerations (money attached to revolving funds, special allotment purposes, etc.). The Branch was also reorganized in order to better meet the new mandate and improve client services. FY 2015-16 is the first year where the CIO Branch is fully functioning with its new operating model, i.e.: with the human and financial resources in place to support the new delivery model.

16. The financial resources allocated to investments in increased functionality to existing applications or to the introduction of a new application or to the IM/IT-enablement of business transformation remains within branches, as does the decision making related to these investments.

Focus of the audit

17. The objective of this audit is to determine whether the actions taken in response to the 2010 Report of the Auditor General of Canada on Aging Information Technology Systems support the Department in managing business applications as a portfolio.

18. The audit focused on the governance and management framework that exists in PWGSC to support the implementation of a portfolio management approach, based on an IM/IT portfolio management framework, IT governance framework, IM/IT Plan, and IT risk profile.

19. More specifically, we examined the IM/IT portfolio management framework; the IT governance framework; the IM/IT Plan; IT risk profile; and application lifecycle management strategies that support the management of the Business Application Portfolio.

20. The scope of the audit focused on the legacy business applications and did not include applications under development or IT infrastructure.

21. More information on the audit objective, scope, approach and criteria can be found in the section "About the audit" at the end of the report.

Statement of conformance

22. The audit conforms with the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program.

23. Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the findings and conclusions in this report and to provide an audit level of assurance. The findings and conclusions are based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. The findings and conclusion are only applicable to the entity examined and for the scope and time period covered by the audit.

Observations

Information management/information technology portfolio management framework has not been fully implemented.

24. In 2011, CIOB developed a Departmental IM/IT Portfolio Management Framework. The objective was to provide an integrated approach to managing IM/IT investments as a portfolio and address the requirements of the Treasury Board of Canada Secretariat (TBS) *Policy on Investment Planning*, as well as the recommendations in the 2010 Report of the Auditor General of Canada on Aging IT Systems. The IM/IT Portfolio Management Framework is based on the VAL IT Framework 2.0, an industry best practice designed to help organizations maximize value of IT-enabled investments at an affordable cost with an acceptable level of risk.

25. As noted in the introduction, in 2013, the Treasury Board of Canada Secretariat (TBS) published the Government of Canada Application Portfolio Management Strategy along with a number of supporting documents such as Government of Canada Application Portfolio Management - Lifecycle Management.

26. We expected PWGSC's IM/IT Portfolio Management Framework would reflect the requirements of the Treasury Board of Canada Secretariat (TBS) Application Portfolio Management Strategy. We also expected PWGSC would manage its portfolio in accordance with the Treasury Board of Canada Secretariat (TBS) Strategy.

27. We found PWGSC's Framework has not been updated since 2011. As a result, it does not reflect the requirements outlined by the 2013 Treasury Board of Canada Secretariat Application Portfolio Management Strategy. We noted the PWGSC Framework does not reflect the new Departmental approach to the management of IM/IT, including the transfer of responsibility and funds from branches to the CIOB to maintain PWGSC applications.

28. Most importantly, we found that the implementation of the Portfolio Management Strategy has been inconsistent, with the implementation of some key elements being limited. The elements where we observed the most significant gaps – application

governance, application lifecycle management, and the IT plan – are discussed in more detail at paragraphs 35 and 46.

29. Addressing these gaps would allow the Department to manage the Business Application Portfolio in accordance with a rigorous portfolio management framework, demonstrating that IT investment decisions are being made based on best practices and the highest priorities of the Department.

30. **Application governance** PWGSC has two governance committees to manage the Departmental Business Application Portfolio. However, we found they are not discharging their mandate in relation to the Business Application Portfolio. This is further discussed beginning in paragraph 35.

31. **Application portfolio information** We found some information and analysis is completed to inform IT investment decision making. However, important information related to mission critical systems and application lifecycle management is not available. These gaps impact the quality of IT investment planning decisions and put the ongoing operations of the Department's Business Application Portfolio at risk.

    i. **Portfolio classification** We found the multi-year IM/IT investment plan presents application investments by Program Alignment Architecture (PAA). This approach meets the classification model set out by the Treasury Board of Canada Secretariat (TBS) Application Portfolio Management Strategy. However, we noted the PWGSC's IM/IT Portfolio Management Framework had not yet been updated to reflect this requirement.

    ii. **Aging IT assessment** We found that at the time of the audit, PWGSC had not formally approved a list of mission critical business applications supporting mission critical services. The approach, including clarifying roles and responsibilities and accountabilities to identify, confirm and approve a list of such applications had not been developed. There were no formal Aging IT Action Plans supporting mission critical applications. Without Aging IT Action Plans to ensure renewal and ever-greening of mission critical, high risk systems, there is a risk the costs of maintaining the systems may not be economical. There is also a risk that critical systems may become unavailable to deliver critical services.

    iii. **Application lifecycle management** We found that applications were assessed regularly on technical condition, business value, and support costs; an assessment was completed in 2012, 2013 and 2014. Of the ten factors recommended to assess technical condition, we found only two (programming language and database) were used. We found the business value score was based on a weighted assessment of its five data elements: efficiency and financial contribution, business criticality, utilization, current effectiveness, and future effectiveness. Support costs as calculated included ongoing hardware, software and labor costs. We also found that applications were categorized by planned management approaches of tolerate, innovate, migrate, and eliminate. However, we found that

Sustainment and Renewal Strategies and Application Reduction Road Maps were not systematically prepared. This is further discussed beginning in paragraph 46.

32. **Planned IT investment** We found the planned financial (discretionary and non-discretionary) investment to be made in IT is included in the Multi-Year IM/IT Investment Plan, which was documented yearly with the exception of the 2012/13-2016/17 iteration. Planned application investment was reported over a five-year planning period, reflecting discretionary and non-discretionary investment as required by the Treasury Board of Canada Secretariat Strategy.

33. **IT plan** We found that the IM/IT Plan included departmental priorities and planned financial investments for a three-year period. However, we found it was not informed by good lifecycle management. More specifically, it did not systematically include Sustainment and Renewal Strategies or Application Reduction Road Maps for the application portfolio, or Aging IT Action Plans for mission critical applications. Finally, in reviewing the Plan, it is not clear to what extent portfolio management information influences investment decisions. Without good lifecycle management, good IM/IT planning is compromised. This is further discussed beginning in paragraph 46.

34. Improvements to the IM/IT Portfolio Management Framework will help provide assurance to application business owners that the Department's IT investments are being managed in a way that employs best practices in portfolio management.

Information technology governance framework is not functioning as per Terms of Reference

35. IM/IT portfolio management requires continual management as it is constantly evolving and involves shared accountability for its success. Shared accountability and decision making cannot be achieved without rigorous application governance between branches and CIOB. IM/IT portfolio management ensures alignment of departmental IM/IT initiatives, services and investments to strategic and operational departmental objectives.

36. Until 2014-2015, the Departmental IM/IT Steering Committee (DISC) and the Director General (DG) Forum were the governance committees set up to drive IM/IT strategies and services. These committees met regularly and discussed issues pertaining to the Business Application Portfolio. The results of the IM/IT portfolio management were presented to Departmental IM/IT Steering Committee (DISC) on an annual basis from 2011 to 2013.

37. Effective 2014-2015, two new committees, the Director General IM/IT Steering Committee (DGIST) and PWGSC IM/IT Steering Committee (PISC) were formed to support IM/IT portfolio management and replace Departmental IM/IT Steering Committee (DISC) and Director General (DG) Forum. The Director General IM/IT

Steering Committee (DGISC) provides PWGSC branches and regions with a forum for business direction and guidance to departmental IM/IT strategies, investments and services, in support of departmental strategic and operational objectives as well as Government of Canada priorities. The PWGSC IM/IT Steering Committee is an Assistant Deputy Minister-level committee with a mandate to direct, oversee, and advance the departmental IM/IT strategic agenda. The PWGSC IM/IT Steering Committee draws on advice and recommendations from the General IM/IT Steering Committee and its supporting committees and working groups.

38. The mandate of the Director General IM/IT Steering Committee, as defined in the Terms of Reference, requires the discharge of the following roles and responsibilities for the Business Application Portfolio:

    i. Recommending to the PWGSC IM/IT Steering Committee the criteria for the economic and strategic value of IM/IT investments, investment prioritization principles, and overseeing the application of these principles in the assessment and prioritization of investment proposals.
    ii. Providing insight on departmental business strategies and plans to support ongoing alignment of the CIOB strategic plan and service portfolio to departmental program priorities and requirements.

39. We concluded that the Director General IM/IT Steering Committee did not discharge its mandate related to the Business Application Portfolio. Based on our review of the records of decisions, we did not find evidence the Committee:

    i. Recommended to the PWGSC IM/IT Steering Committee the criteria for prioritizing IM/IT investments, as the criteria were not approved or in place until April 2015. As a result the criteria were not used to prioritize investments, and there hasn't been any oversight by the Committee of IM/IT investment proposals using the criteria.
    ii. Provided insight into IM/IT portfolio management. We noted that IM/IT portfolio management, as it relates to the Business Application Portfolio, was only tabled twice over a period of 12 months. In the first instance (April 2014), the approach to Technology Modernization was presented. A year later (April 2015), criteria to prioritize IM/IT investments were presented and agreed upon by the Director General IM/IT Steering Committee (DGIST). No other strategies in relation to application portfolio management were presented.
    iii. Was informed by important lifecycle management information or informed on risk mitigation strategies related to the Business Application Portfolio, as discussed further below.

40. The mandate of the PWGSC IM/IT Steering Committee, as per the Terms of Reference, requires the discharge of the following roles and responsibilities for the Business Application Portfolio:

i. Providing strategic direction of departmental IM/IT investments and prioritization of activities leading to the rationalization of departmental business applications to ensure alignment with departmental and governmental priorities and directions.

ii. Overseeing the application of prioritization principles for IM/IT investment proposals and ensuring investment proposals meet the criteria for the economic and strategic values of IM/IT investments.

iii. Approving the prioritization of IM/IT investments recommended by the Director General IM/IT Steering Committee.

41. We concluded the PWGSC IM/IT Steering Committee did not adequately discharge all of its mandate related to the Business Application Portfolio. Based on our review of the records of decisions, we did not find evidence the Committee:

    i. provided strategic direction of departmental IM/IT investments leading to the rationalization of departmental business applications.

    ii. oversaw application of prioritization principles for IM/IT investment proposals and ensured investment proposals met the criteria for the economic and strategic values of IM/IT investments, since the criteria were not approved until April 2015 and no the PWGSC IM/IT Steering Committee meeting has taken place since April 2014.

    iii. approved prioritization of IM/IT investments recommended by the Director General IM/IT Steering Committee or alignment of departmental IM/IT investments of the branches. Specifically related to the Business Application Portfolio, the PISC could not meet their mandate requirements of the TOR, since the advice and recommendations from the Director General IM/IT Steering Committee (DGIST) were limited and the prioritization of IM/IT investments was not supplied to the PWGSC IM/IT Steering Committee (PISC) by the Director General IM/IT Steering Committee, as it is currently a work in progress. This demonstrates that critical application portfolio information used to drive application investment prioritization and risk planning at the enterprise level is not being managed adequately.

42. As such, we did not find evidence the Director General IM/IT Steering Committee or the PWGSC IM/IT Steering Committee provided influence over IM/IT management, investment planning, and risk management. More specifically, prioritization criteria were not developed until 2015, important application lifecycle management information and analysis was not available to the Committee, and risk reporting had not been systematically presented.

43. We were informed that many bilateral discussions occurred between senior executives outside of the PWGSC IM/IT Steering Committee. Partner Relationship Directors and Product Life Cycle Managements from CIOB maintain ongoing discussions with their

counter parts in the Branches. These roles were introduced as part of the reorganization to better meet the new mandate and improve client services. Further, Partner Service Agreements were established with every branch outlining change and transform activities, along with a commitment from partners to decommission applications no longer having business value.

44. While this model contributes to managing the joint accountabilities between CIOB and branches for business applications and supports investment planning and implementation of those plans, it does not meet the expectations for governance at the Department-wide level that is required for management of the business applications as a portfolio.

45. Strengthening the IT governance framework will help support IM/IT investment decisions on a portfolio basis and will provide direction for long term strategies to meet current and emerging priorities for the Department.

Investment decisions captured in the IM/IT Plan are not systematically based upon application lifecycle management methodology and Aging IT Action Plans

46. Application lifecycle management, which begins with a TIME assessment, includes assignment of a planned approach to manage applications; as well, Sustainment and Renewal Strategies and Application Reduction Road Maps form a key part of the information and analysis that feeds IM/IT planning process. These, along with Aging IT Action Plans for mission critical applications and the PWGSC's Multi-Year IM/IT Investment Plan, inform investment planning decisions made by the Department and governance committees which are reflected in the IM/IT Plan.

47. PWGSC has adopted the industry recognized Gartner TIME assessment framework as proposed by the Government of Canada to inform the planned approach for managing business applications based on technical condition, business value, and support costs. As per the Gartner TIME model, the planned approach to manage each application is categorized as either **Tolerate**, **Innovate**, **Migrate**, or **Eliminate**.

- **Tolerate** applications remain in-service and deliver medium to low business value; the costs, resources use and risks are acceptable.
- **Innovate** applications deliver high to medium business value and are candidates for investment, innovation or integration to increase their effectiveness.
- **Migrate** applications deliver high business value but have poor use of IT resources that require immediate attention for remediation or migration.
- **Eliminate** applications deliver low business value, poor use of IT resources, and should be eliminated and removed from being in-service.

48. This approach, which considers the technical condition and business value, in the context of support costs, allows an assessment of the limited lifespan of IT systems that must be sustained, renewed, or eliminated.

49. Application lifecycle management coupled with Aging IT Action Plans enables enterprise oversight of applications, and allows departments to focus on application management strategies that are both economical and support the continuity of services. Sustainment and Renewal Strategies, Application Reduction Road Maps, and Aging IT Action Plans for mission critical applications outline the strategy for managing these business applications on a go forward basis.

50. We expected that the application lifecycle management methodology along with Aging IT Action Plans would consistently drive investment decisions. More specifically, we expected that the lifecycle of applications from a business and technology perspective would be assessed regularly. Further, we expected the results of this assessment, along with Sustainment and Renewal Strategies, Application Reduction Roadmaps, and Aging IT Action Plans for mission critical applications, would be presented and discussed at governance committees to provide guidance and drive investment decisions. Finally, we expected these would be reflected in the PWGSC's IM/IT Plan.

51. As noted previously, we found that PWGSC applications were assessed regularly according to the TIME assessment framework, although not all technical elements were assessed. However, we did not find Sustainment and Renewal Strategies, Application Reduction Roadmaps, or Aging IT Action Plans for mission critical applications. Further, we did not find evidence that the results of lifecycle management or Aging IT Action Plans informed governance committees or were reflected in the IM/IT Plan.

52. Based on the results of applying the TIME assessment framework, a number of applications had been identified as candidates for elimination. We found that the Department has reduced the number of business applications across branches at PWGSC from 441 applications in 2010 to 313 in 2014.

53. However, we also found limited modernization of the remaining 313 applications has been delivered. Of these, 142 applications have been identified as candidates for migration because they remain important in delivering high business value services to internal and external clients but need to be upgraded. However, we are unaware of the planned next steps for these applications as no Sustainment and Renewal Strategies have been developed.

54. We also found the TIME assessment results were presented to governance committees in 2012. However, there is no evidence that subsequent assessment results were presented to those committees in 2013 and 2014. In addition, as key deliverables from

application lifecycle management such as Sustainment and Renewal Strategies, Application Reduction Road Maps, and Aging IT Action Plans for mission critical applications have not been prepared, nor were they presented to governance committees. Further, there is no evidence lifecycle management results are reflected in the IM/IT Plan.

55. Information obtained through the application of the lifecycle management methodology and the Aging IT Assessment is important to inform governance committees in their investment decision making and to influence IM/IT planning. Without that information, decisions are being made on incomplete information. Enhancing the information and analysis resulting from lifecycle management will assist in ensuring IT investment decisions are made based on highest priorities for the entire portfolio.

Information technology risk management can benefit from better monitoring of strategies

56. The Report of the Auditor General of Canada on Aging IT Systems defined aging IT risks as:

> ***"risks [that] may affect security or restrict the way the government conducts its business because systems cannot be easily updated to respond to changing business needs flowing from new laws, regulations, or industry standards. The most damaging risk is that an aging critical system could fail and prevent the government from delivering key services to the public."***

57. To manage aging IT risks, the audit report recommended that PWGSC develop an action plan for each significant aging IT risk. These plans were to include specific strategies, key activities, deliverables, and timelines to manage these risks. The individuals responsible for managing these plans were to report progress regularly to senior management.

58. PWGSC's response was twofold. It agreed to refresh its corporate risk profile to validate corporate risks, including those relating to aging IT applications. It also agreed to conduct an IT specific risk profile exercise to develop a departmental IT risk profile.

59. Although aging IT was identified as a significant risk by PWGSC in its Corporate Risk Profile for 2012-2013 and 2013-2014, it was removed in the 2014-2015 Corporate Risk Profile as it was determined to be an operational-level risk rather than a corporate-wide risk. Reducing the aging IT application risk to an operational level reduces the visibility and level of oversight from the management committees and reduces the ability of the branches to direct the long term sustainability for critical applications and IM/IT investments as this risk is deemed operational in nature.

A. Public Works and Government Services Canada information technology risk profile (Department-level)

60. In accordance with the commitment made in response to the Auditor General report, we expected PWGSC would develop an IT risk profile and update it regularly. This includes identification of risks, assignment of risk owner, and development of risk response strategy, which is monitored and modified as necessary.

61. We found that a Departmental IT Risk Profile has been developed. An IT Risk Profile Group was set up, and in collaboration with a special Director General Committee, they met and interviewed branches across PWGSC to determine the key IT risks to the Department. Based on this work, in 2012, a PWGSC IT Risk Profile was developed that identified risks and risk responses.

62. However, we found risk owners have not been identified for significant risks, and reporting on risk responses has been inconsistent; there has been no formal reporting or monitoring of risks identified from within the PWGSC IT Risk Profile. Further, we found that the Risk Profile had not been updated since 2012.

B. Chief Information Officer Branch information technology risk profile (Branch-level)

63. As per the PWGSC Risk Management Guide, which was developed in accordance with the Treasury Board of Canada Secretariat Framework for the Management of Risk, each Branch is required to develop a Branch Risk Profile as part of its risk management process. Branch Risk Profiles are to identify branch risks, risk owners, risk responses, and the criteria to assess the impact of the branch risk responses. The status of risk responses is to be recorded in the Deputy Minister Scorecard on a semi-annual basis.

64. We expected CIOB to develop a Branch Risk Profile that identified the risks specifically related to aging IT applications. We also expected that the risk profile would identify risk owners, risk responses, and the criteria to assess the impact of the branch risk responses. Finally, we expected that the status of risk responses would be recorded in the Deputy Minister Scorecard on a semi-annual basis.

65. We found the CIOB has developed an IT Risk Profile that is updated annually. It identifies risks related to aging IT applications. More specifically, one identified risk is that the integrity of PWGSC's aging assets and systems may be compromised.

66. Risk responses are identified and risk owners are assigned to each risk response. However, we noted key activities, deliverables, and timelines have not been clearly specified nor are they measurable.

67. Currently, reporting of aging IT risks is found within the Deputy Minister Scorecard as a portion of an aggregated score. This score measures the percentage of activities for IM/IT modernization completed during the fiscal year. As the risk responses are not measurable, it is not possible to gauge changes in levels of risk or whether risk responses have been completed.

68. As a result, information on risks and their mitigation is not available to be shared with governance committees to inform decision making. Further, we did not find evidence that risk management activities are reflected in the IM/IT Plan. Clear and measurable risk responses that are monitored and reported on help ensure IT risks are well managed and appropriately inform decision making and planning.

Conclusion

69. We found that the CIOB has taken a number of actions in response to the 2010 Report of the Auditor General of Canada on Aging IT Systems to support the Department in managing business applications as a portfolio. However, we noted a number of areas for improvements in application governance, application management, and IT plan.

70. To address the requirement of the Treasury Board of Canada Secretariat(TBS) *Policy on Investment Planning* and the recommendations from the Auditor General report, PWGSC published an IM/IT Portfolio Management Framework. Some progress has been made with PWGSC's adoption of IM/IT portfolio management. More recently, the Treasury Board of Canada Secretariat (TBS) developed an Application Portfolio Management Strategy. PWGSC's IM/IT Portfolio Management Framework needs to be updated to reflect the requirements of the Treasury Board of Canada Secretariat Application Portfolio Management Strategy. Although some key elements of the Strategy have been implemented, some important gaps in implementation remain, particularly in terms of application governance, lifecycle management, Aging IT Action Plans, and the development of the IM/IT Plan.

71. Governance committees play an important role in the implementation of successful IM/IT portfolio management. The PWGSC IM/IT Steering Committee (PISC) and the Director General IM/IT Steering Committee (DGISC) were set up to drive IM/IT strategies and services. These committees have not fulfilled their mandates related to business application portfolio management, as defined in their respective Terms of References. IM/IT portfolio management may not have been adequately discussed or progressed at the governance committee level, and there was no evidence that IM/IT portfolio management informed IM/IT investment decision making.

72. The application lifecycle management methodology provides information on the lifecycle status of applications and their planned management approaches to help inform decision making. PWGSC applications were found to be assessed regularly

according to the TIME assessment methodology. The CIOB has used the results to consolidate and reduce the number of applications in its portfolio. However, Sustainment and Renewal Strategies and Application Reduction Roadmaps were not prepared. Most significantly, we did not find evidence application lifecycle information or Aging IT Action Plans were used to drive IM/IT investment decisions.

73. In accordance with the commitment made in response to the Auditor General report, PWGSC refreshed their Corporate Risk Profile to include aging IT applications, and developed an IT Risk Profile. Although aging IT was identified as a significant risk by PWGSC in its Corporate Risk Profile in 2012-2013 and 2013-2014, it was removed in 2014-2015 as it was considered to be an operational risk. Risk categorization of aging IT applications as operational reduces management oversight for these risks and, as they are not discussed at the appropriate level, it does not allow the departments a forum to manage the long term strategy or IM/IT investments for these aging IT applications.

74. PWGSC developed a department-wide IT Risk Profile in 2012, which identified risks and risk responses. Reporting on risks was inconsistent, and there has been no formal reporting of risks and risk responses from within the IT Risk Profile. Furthermore it has not been updated since its inception. As a result, there is no evidence that risk mitigation strategies are being monitored or that risk management is informing IM/IT investment decision making.

75. The CIOB developed an IT Risk Profile that is updated annually and identifies risks related to aging IT applications. Risk responses are identified and risk owners are assigned to each risk response. However, key activities, deliverables, and timelines have not been clearly specified nor are they measurable. Therefore, it is not possible to gauge changes in levels of risk or whether risk responses have been completed. As a result, information on risks and their mitigation is not available to be shared with governance committees to inform decision making. Clear and measurable risk responses that are monitored and reported on help ensure IT risks are well managed and appropriately inform decision making and planning.

Management response

Management has had the opportunity to review the report, and agrees with the conclusions and recommendations found therein. Management also developed a Management Action Plan to address these recommendations.

Recommendations and Management Action Plan

Recommendation 1: The Chief Information Officer, Chief Information Officer Branch should update and fully implement a PWGSC Portfolio Management Framework.

Management Action Plan 1: CIO Branch will review, update, and implement Application Portfolio Management (APM) in accordance with TBS framework. This will include:

> **Management Action Plan 1.1:** Realigning client delivery functions i.e. project management to Service Management and allowing Product Management team to focus on conduct of APM, release management, and continuous service delivery model and tools improvement.
>
> **Management Action Plan 1.2:** Documenting and communicating to DG and ADM level committees the required annual APM cycle including elements, accountable organizations, deliverables, and links to other activities such as departmental IM/IT investment plan, risk mitigation, and governance.
>
> **Management Action Plan 1.3:** Reviewing the TBS framework for Application Portfolio Management, mapping to current CIO Branch practices in order to identify gaps, e.g. applications that have not yet been assessed or partially assessed.
>
> **Management Action Plan 1.4:** Presenting APM findings to the DG and ADM level committees, highlighting the gaps and priorities. This will garner support to close the gaps and address the aging IT priorities highlighted through the APM exercise. For example, applications classified as "Migrate" with higher risk due to aging infrastructure should receive higher priority for remediation.

Recommendation 2: The Chief Information Officer, Chief Information Officer Branch should enhance the governance structure that supports IT investment.

Management Action Plan 2: CIO Branch will ensure the departmental IM/IT governance committees are leveraged and are core to the revised IM/IT Investment Planning and Portfolio Management Framework and related processes. This will entail re-launching the IM/IT Governance by:

> **Management Action Plan 2.1:** Establishing an annual schedule of meetings for both the ADM and DG level committees.
>
> **Management Action Plan 2.2:** Ensuring the ADM and DG level committee understand their role by reviewing/revising the terms of reference for both the ADM and DG-level committees to ensure that the committees are supporting the new branch operating model.
>
> **Management Action Plan 2.3:** Engaging the ADM and DG level committees in reviewing the Department's IM/IT Investment Plan prior to DM-level Investment Management Board decisions.

Management Action Plan 2.4: Providing a bi-annual report on change and transform activities and investments, in support of departmental IM/IT prioritization.

Recommendation 3: The Chief Information Officer, Chief Information Officer Branch should provide relevant information, such as Sustainment and Renewal Strategies, Application Roadmaps, and Aging IT Action Plans for mission critical applications, to support decision making related to investment planning and management decisions.

Management Action Plan 3: CIO Branch will document and communicate outcomes from the on-going APM analysis including results of the TIME (Tolerate, Innovate, Migrate and Eliminate) to support decision making related to Application Roadmaps, investments planning, and risk management and mitigation strategies. This will include:

Management Action Plan 3.1: Identifying, documenting and communicating mission critical and essential applications.

Management Action Plan 3.2: Documenting and communicating current TIME results as input to the annual IM/IT Investment Plan including governance, risk management, and mitigation. For example, applications classified as "Migrate" with higher risk due to aging infrastructure should receive higher priority for remediation.

Management Action Plan 3.3: Documenting and communicating planned individual branches' investment in "Change" portfolio in support of priority setting (as per actions of Recommendation 2 above).

Management Action Plan 3.4: Provide the Partner's Application Portfolio in Partner Service Agreements.

Management Action Plan 3.5: Provide quarterly updates on actual costs by application in the Partner Service Agreements.

Recommendation 4: The Chief Information Officer, Chief Information Officer Branch should strengthen the risk management processes related to legacy business applications.

Management Action Plan 4: CIO Branch will leverage the outcome from the TIME analysis to document, publish, and communicate required investment and activities related to legacy business applications in support of governance and decision making. This will include:

Management Action Plan 4.1: Documenting and communicating outcomes from the TIME analysis.

Management Action Plan 4.2: Leveraging the governance in Recommendation 2 to secure required direction and decision to support proposed risk management and mitigation strategies.

About the audit

Authority

This engagement was included in the Public Works and Government Services Canada (PWGSC) 2013-2018 Risk-Based Audit and Evaluation Plan.

Objective

The objective of this audit is to determine whether the actions taken in response to the 2010 Report of the Auditor General of Canada on Aging Information Technology Systems support the Department in managing business applications as a portfolio.

Scope and approach

The audit covered activities for the last three fiscal years (FY) – from FY 2012-2013 to FY 2014-2015.

The audit focused on the governance and management framework that exists in PWGSC to support the implementation of a portfolio management approach based on an IM/IT portfolio management framework, IT governance framework, IM/IT plan, and IT risk profile.

The scope of the audit focused on the legacy business applications and did not include applications under development or IT infrastructure.

This audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

Criteria

The audit criteria used were developed based upon the Spring 2010 Report of the Auditor General of Canada on Aging Information Technology Systems and *Control Objectives for Information and Related Technology* (COBIT).

The criteria were as follows:

- Framework, policy, and process are in place to support a departmental multi-year IM/IT investment plan based on portfolio management approach.

- A multi-year IM/IT investment plan based on portfolio management approach has been developed, is reviewed annually, and complements the integrated investment plan.

- Risks relating to Business Application Portfolio are adequately identified and managed through the IT specific risk profile.

- Strategies to address business continuity requirements in line with the key systems are in place and functioning as intended.

Audit work completed

Audit fieldwork for this audit was substantially completed on April 20, 2015.

Audit team

The audit was conducted by members of the Office of Audit and Evaluation, overseen by the Director Internal Audit, and under the overall direction of the Chief Audit and Evaluation Executive.

The audit was reviewed by the quality assessment function of the Office of Audit and Evaluation.