



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Canada

Horizontal Internal Audit of Information Technology Asset Management in Small Departments and Agencies

Published: 2011-00-07

© Her Majesty the Queen in Right of Canada,
represented by the President of the Treasury Board, 2011

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT66-43/2010E-PDF
ISBN: 978-0-660-25532-3

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Vérification interne horizontale de la gestion des actifs des technologies de l'information dans les petits ministères et organismes



Horizontal Internal Audit of Information Technology Asset Management in Small Departments and Agencies

Horizontal Internal Audit of Information Technology Asset Management in Small Departments and Agencies

April 2010

Contents

[Executive Summary](#)

[Why this is important](#)

[Key findings](#)

[Conclusion](#)

[Statement of Assurance](#)

[Background](#)

[Audit Objectives, Scope, and Approach](#)

[Objectives and scope](#)

[Audit approach](#)

[Detailed Findings and Recommendations](#)

[Finding 1: IT governance structures and planning](#)

[Finding 2: Planning IT acquisitions](#)

[Finding 3: Monitoring processes](#)

[Management Action Plans](#)

[Appendix A: Audit Criteria](#)

[Appendix B: Departments and Agencies Included in the Audit Engagement](#)

[Appendix C: Ranking of Recommendations](#)

[Appendix D: Links to Applicable Frameworks, Policies, and Directives](#)

Executive Summary

The objective of this audit was to determine whether the management and control structures in place in small departments and agencies (SDAs) provide an effective framework for managing information technology (IT) assets. We also examined the policies and the guidance provided by the Treasury Board of Canada Secretariat (TBS) to SDAs in this regard.

Why this is important

The Government of Canada spends a significant amount of its annual budget on IT assets and services. As well, IT is an essential component of the government's strategy to address the challenges of increasing productivity and enhancing services to the public for the benefit of citizens, businesses, taxpayers, and employees. For these reasons, it is important to have assurance on the extent to which appropriate structures are in place for managing IT assets and risks, acquiring these assets, and monitoring their performance. This audit is intended to provide that assurance.

Key findings

SDAs have established governance structures appropriate to the size and scope of their IT activities. We found evidence of short-term IT investment planning in most SDAs; however, many of the SDAs included in our audit had not developed long-term plans as required by the Treasury Board *Directive on Management of Information Technology*. Nevertheless, respecting the requirements of the directive in this area may be more demanding than the value added for some SDAs, given the size and scope of their IT-related activities. As such, an opportunity exists for TBS—the central agency responsible for setting IT policy—to work with SDAs to examine if existing IT policies are consistent with the IT asset management risks faced by SDAs.

There was evidence that SDAs considered the budget required for acquisition of IT assets during the annual budget planning cycle. However, many SDAs could not demonstrate that they were prioritizing their planned IT acquisitions on the basis of the life cycle of assets or other risks. Accordingly, we cannot provide assurance that SDAs have spent their technology dollars on IT items of highest priority in terms of risk or operational needs or that they have replaced items only when necessary and not before the end of their useful life.

The *Policy on Management of Information Technology* requires departments and agencies to use shared assets and IT-related services where appropriate and when available; however, certain legislative and other barriers tend to discourage SDAs from complying with that policy. A working group at the Office of the Comptroller General of Canada (OCG) is currently working on addressing this and other related issues. Nevertheless, we found evidence of one SDA that had successfully adopted a shared IT asset model in collaboration with a large department.

Most SDAs were not measuring the performance of their IT assets as required by the Policy Framework for Information and Technology. None of the SDAs had developed appropriate targets and indicators—the basic prerequisites to measuring performance. We noted that TBS has developed some preliminary performance indicators in consultation with SDAs. However, these indicators have not been formally communicated to relevant stakeholders in SDAs. As such, we saw no evidence of these being used by the SDAs included in our audit.

Conclusion

Overall, we are satisfied that, given the scale and scope of the activities within the SDAs included in our audit, the management and control structures in place provide an effective framework for managing IT assets.

Statement of Assurance

This audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada and the International Standards for the Professional [\[1\]](#)

Brian M. Aiken CIA, CFE
Assistant Comptroller General
Internal Audit Sector, Office of the Comptroller General of Canada

Background

The Treasury Board *Policy on Internal Audit* requires the Comptroller General to lead horizontal audits in small departments and agencies (SDAs). Horizontal audits assess those risks that transcend individual departments, focusing on the state of governance, controls, and risk management across government. This report presents the results of the *Horizontal Internal Audit on Information Technology Asset Management in Small Departments and Agencies*. Various Treasury Board policies and directives, which are briefly outlined below, guide the government's IT asset management practices.

The objectives of the *Policy on Management of Information Technology* are to achieve efficient and effective use of IT to support government priorities and program delivery, to increase productivity, and to improve services to the public. The expected results of these objectives include clear roles and responsibilities for IT management in the Government of Canada, increased use of common or shared IT assets and services, and enhanced management of IT across the government to ensure that IT supports program delivery and provides value for money.

The Policy Framework for the Management of Assets and Acquired Services, among other things, outlines key asset management principles, including the use of a life cycle approach when planning acquisitions such as IT assets.

The *Directive on Management of Information Technology* sets out specific requirements for the governance and management of IT and emphasizes the need for a long-range (five-year) IT plan that is integrated with the annually reviewed and updated departmental investment plan.

The *Policy on Investment Planning – Assets and Acquired Services* requires departments and agencies to develop investment plans that are aligned with their strategic direction and to take asset performance (including cost and risk) into consideration.

The SDA community in the federal government is extremely diverse, varying in, for example, organizational structure and size, budget, nature of work, and relationship with larger departments. The budgets of SDAs do not exceed \$300 million per year, while personnel gross expenditures represent approximately 65% of expenditures. Their full-time equivalents vary from 10 to 500 employees. These factors contribute to the nature of the financial systems and controls that SDAs have implemented for decision making and accountability.

Audit Objectives, Scope, and Approach

Objectives and scope

The objective of this audit was to determine whether the management and control structures in place in SDAs provide an effective framework for managing IT assets.

The scope of this audit included IT asset management systems and practices in place in a sample of SDAs as of December 2009. The audit focused on IT governance structures, IT acquisition planning processes, the extent to which SDAs had taken advantage of opportunities to share IT assets and services with other organizations, and the processes used to measure the performance of their IT assets. We also examined the actions and the guidance provided by TBS to SDAs in this regard.

Audit approach

The audit team consisted of internal auditors from the Internal Audit Sector of the OCG. The audit was conducted in three phases.

Phase 1 – planning

To focus the audit on the appropriate areas of risk, we performed an environmental scan of IT asset management in the Government of Canada. The scan consisted of the following: a review of the key government-wide policies and directives relating to IT; interviews with senior IT managers from TBS (the government's central agency responsible for designing and implementing Treasury Board policies) and Public Works and Government Services Canada (PWGSC) (the government's primary common service provider for IT and the government's central procurement agent); a review of the literature on key IT asset management risks and controls; an analysis of the IT asset management systems and practices in place in two SDAs; and a review of best practices outlined in the Control Objectives for Information and related Technology (CobiT) framework. We also discussed our audit with individuals from the Office of the Auditor General who are involved in the audit of aging IT systems to ensure that our work did not duplicate the audit work of other assurance providers. See Appendix A for a list of the criteria that guided our

To select the sample of organizations for our audit, we analyzed the results of the annual assessment of IT management practices in government departments, the prior participation of SDAs in other horizontal audits, and the level of spending of individual SDAs. This exercise ensured that our final selection was based on performance and spending factors and included a range of organizations. As a result of this analysis, we chose 11 SDAs. See Appendix B for a list of the organizations included in our sample.

Phase 2 – examination

We began this phase by interviewing personnel responsible for managing IT assets in the selected SDAs. We then examined supporting documents to corroborate the information collected from the interviews. These documents included departmental IT or investment plans, IT asset acquisition plans, organizational charts, job descriptions, and reports on IT performance and inventory management.

Fact sheets were prepared for each of the SDAs and were confirmed with them before the audit team began to write the report.

The OCG carried out interviews with TBS officials involved in government-wide management of IT assets. The OCG also reviewed documents and tools that support SDAs in managing their IT assets, including policies and guidance materials.

In addition, the OCG consulted with the PWGSC to understand its role as a common service provider of IT services and to verify facts related to its mandate. PWGSC, however, was not included in the scope of this audit.

Phase 3 – reporting

Following the detailed examination phase of the audit, we consolidated our findings to identify any horizontal issues. Finally, we drafted our final horizontal internal audit report.

Detailed Findings and Recommendations

Finding 1: IT governance structures and planning

In most SDAs, the governance structures for managing IT assets were reasonably designed and implemented.

Context

A well-defined governance structure is a prerequisite to enabling an organization to invest its IT resources effectively. A long-range IT plan is also important. It sets out the IT objectives, ensures that investments align with departmental and government-wide objectives, and reduces the likelihood of investing in low-priority technology assets. When IT investments are guided by an organization-wide IT strategy, the risk of acquiring incompatible or unsupportable technologies is

We reviewed the roles and responsibilities of the IT governance structures in SDAs included in our audit to determine whether they were appropriate. We also reviewed departmental IT plans to determine the extent to which they were linked to departmental business plans and government-wide objectives. Lastly, we assessed departmental IT plans to establish how far the IT plans projected into the future.

Governance structures

SDAs had established governance structures appropriate to the size and scope of their IT activities. Most had a committee composed of IT and general management that reviewed and approved IT investments. In most SDAs, a senior person had been formally assigned responsibilities for managing IT assets.

Long-term IT planning

The *Directive on Management of Information Technology* requires all departments and agencies to develop long-term IT plans with a minimum five-year horizon. It also requires that long-term IT plans be aligned with the department's business objectives to increase the likelihood that IT investments will be of

Although we found evidence of short-term IT planning in most SDAs, many could not demonstrate that they had carried out long-term planning. In addition, many could not demonstrate in their IT plans how proposed IT investments would support departmental and government-wide objectives. We noted that some SDAs did not view IT as central to their core mandate. In other SDAs, investment in IT was relatively small. As a result, many SDAs were managing IT on a day-to-day basis, which would account for the general lack of long-term IT planning across these organizations.

Given the size and scope of IT assets in some SDAs, respecting the requirements of government-wide policies in this area may be more demanding than the value added. Making risk-informed decisions about policy compliance may be appropriate in this area. The *Directive on Management of Information Technology*, as well as related policy instruments, does not address this issue.

Recommendation

1. TBS, in collaboration with SDAs, should determine whether government-wide IT policies governing the management of IT in SDAs are consistent with the IT

Finding 2: Planning IT acquisitions

Most SDAs were not prioritizing their IT asset acquisitions. In addition, there was limited evidence of IT asset sharing by SDAs.

Context

Effective planning for IT acquisitions ensures that investments support the goals of the organization and that technology dollars are directed to those assets that are most important to its operations. Planning should incorporate a life cycle approach to IT assets, taking into account, for example, the risks associated with a decision to replace an aging asset or to extend its life. Planning should also include consideration of shared IT assets where available

We reviewed the long-range asset acquisition plans to determine whether they were linked to the departments' business plans, and we assessed the extent to which SDAs had prioritized their planned IT asset acquisitions. We examined the extent to which SDAs had considered the life cycle of IT assets in their planning process and whether that process accounted for IT risk. Lastly, we assessed the extent to which SDAs had considered the use of common or shared IT assets and services with other organizations when planning their IT acquisitions.

Planning and prioritizing IT asset acquisitions

We found that SDAs had carried out some level of planning for the acquisition of IT assets. Most of this work was undertaken as part of the annual budget planning cycle, when SDAs establish their IT infrastructure requirements and plan their IT acquisitions for the next fiscal year.

We found that most SDAs in our sample had not prioritized their planned IT acquisitions. Some could not demonstrate that they had considered the life cycle of assets in planning for IT acquisitions. Others could not demonstrate that their IT acquisition plans had considered the risk associated with any decision to replace a given asset. As a result, we have no assurance that SDAs spent their technology dollars on the IT items of highest priority or that they replaced items only when necessary and not before the end of their useful life.

A key reason for these weaknesses in planning for IT acquisitions is that most IT units in SDAs only submit a cost estimate for planned IT acquisitions to their finance units for their annual budgeting cycle. Although this approach does indicate how much money should be set aside to acquire assets, it does not indicate the specific IT assets that the organization will acquire with the allotted funds or whether these assets are the highest priority in terms of risk or operational needs.

Sharing IT assets and services

We found that the majority of SDAs included in our audit considered shared IT infrastructure on a case-by-case basis. Evidence of actual sharing of IT assets was limited. Generally, each SDA had established its own infrastructure, which paralleled the infrastructure of other organizations. Parallel infrastructures present an opportunity for rationalization or sharing that should be further explored.

There are barriers to interdepartmental sharing

We noted that there are a number of barriers to interdepartmental sharing of IT assets and services.

For example, legislative barriers exist that prevent departments from sharing assets or providing services to other departments. In addition, privacy laws may prohibit sharing of information. A working group at the OCG is currently working on addressing both of these issues.

SDAs and the common service provider for IT have indicated that there are some barriers to the use of shared services and assets provided by the common service provider. Foremost, it can be more expensive for an SDA to adopt a shared asset or a shared service solution provided by the common service provider than to develop its own. In addition, since each SDA defines IT services differently and allocates asset costs to services according to its own model, it can be difficult to compare the costs of doing IT work within a department with a shared services model. Finally, some SDAs have concerns that service levels could decrease if they were to use a shared solution versus an in-house solution.

The scope of this audit did not include an assessment of whether the above concerns are valid. Nevertheless, these issues need to be addressed in order to determine the extent to which they may be discouraging SDAs from considering shared IT asset and service solutions.

Best practice in sharing IT assets

We noted that one SDA had organized its technology services to reduce redundancy of IT resources and assets by using shared IT assets. This particular SDA has signed a Memorandum of Understanding with a large department to receive IT services, and it has a shared vote on IT spending with that department. The SDA participates in the IT planning cycle of the large department, where it makes known its objectives. Under this arrangement, the large department owns and manages all "back office" IT assets and resources (for example, servers, back office software, LAN/WAN infrastructure, and IT staff) other than desktops. As a result, the SDA

does not maintain these IT assets or related staff. This arrangement eliminates duplication of IT assets and resources for the SDA.

We considered this arrangement to be a best practice. It transfers the management of an activity that is not a core competence of the SDA to a third party while establishing a mechanism to ensure that the level of service will remain as high as if these activities were carried out in-house. The SDA and the large department are in the process of developing a Service Level Agreement to formalize this arrangement.

Recommendations

2. SDAs should ensure their IT plans for proposed acquisitions address areas of highest priority in terms of risk, life cycle of assets, or operational needs.

3. TBS should identify and resolve the barriers that limit the adoption of shared IT assets and services by SDAs where appropriate. This activity should include an examination of parallel infrastructures that present an opportunity for rationalization or sharing.

Finding 3: Monitoring processes

Most SDAs did not have indicators for measuring the performance of their IT assets.

Context

To ensure that IT assets deliver maximum value to the organization, SDAs need to know, for example, whether IT assets are underutilized or over-utilized, what the failure rates are, and whether cost targets are being met. Monitoring and measuring the performance of these and other aspects of IT provide valuable information that SDAs can use to identify and deal with problem areas. They also provide information on which SDAs can base decisions about future IT acquisitions.

Good stewardship requires that an organization track its IT assets to verify their location and condition. The output of asset tracking systems can also provide early warning signs of missing assets. Software licences should also be tracked because organizations have a legal obligation to comply with software licensing agreements.

We reviewed the processes used to measure IT asset performance. We verified whether SDAs had defined financial and non-financial performance indicators and the extent to which they were measuring and reporting performance against these indicators. We interviewed senior management within SDAs to understand how assets were tracked. Finally, we reviewed inventory reports for evidence of a system for tracking software licences.

Tracking assets

Most SDAs had well-defined processes for tracking and accounting for their IT assets. As well, most SDAs periodically inventoried their hardware and software assets to ensure accountability and compliance with software licensing agreements.

Non-compliance with policy on measuring IT performance

The majority of SDAs were not able to demonstrate that they had an adequate process for measuring and reporting on the performance of IT assets as required by the Policy Framework for Information and Technology. None of the SDAs had defined objective, quantitative performance (financial or non-financial) targets, such as cost overruns, service levels, and downtime. Some SDAs had considered subjective, qualitative data, such as users' opinions on the performance of their computers on different days, when making IT asset purchase decisions. However, such data may not provide useful information for decision making because the data are subjective and offer only a limited picture of the performance of an asset.

Rationale for non-compliance with policy on measuring IT performance

The reasons for not measuring IT performance varied. Some SDAs told us that their small-scale use of IT assets did not warrant a comprehensive process for monitoring and measuring IT performance. Others noted that they had competing priorities that were more important relative to measuring IT performance. However, without some form of objective performance measurement, the ability to make

TBS, in consultation with SDAs, has developed some preliminary performance indicators for IT assets; however, they have not been formally communicated to all relevant stakeholders in SDAs. As such, we saw no evidence of these being

Recommendations

4. SDAs should develop processes for measuring the performance of IT to ensure that they have objective information to support their management decisions about IT.

5. TBS should ensure that the performance indicators that have been developed for IT have been communicated appropriately to those who are responsible for collecting data and measuring performance.

Management Action Plans

The findings and recommendations of this audit were presented to TBS and the eleven SDAs included in the scope of the audit.

The OCG's Internal Audit Sector asked TBS and the SDAs included in the audit to prepare detailed Management Action Plans addressing the recommendations in this report.

The Internal Audit Sector of the OCG will follow-up on the Management Action Plans proposed by the SDAs and the Chief Audit Executive of TBS will follow up on the Management Action Plans proposed by TBS. The purpose of this follow up is to ensure that the Management Action Plans have been successfully implemented to address underlying risks. The respective audit committees will periodically receive reports on the status of management actions taken where Management Action Plans are in place.

Deputy heads of SDAs not included in the scope of this audit are encouraged to consider the results of this horizontal internal audit and develop Management Action Plans as necessary.

Appendix A: Audit Criteria

Criteria	Sub-Criteria
IT governance structures are in place to provide strategic direction for IT asset management.	<ol style="list-style-type: none">1. Roles and responsibilities are defined and communicated (e.g. leadership, control over acquisition, monitoring, and oversight).2. Policies and procedures are defined and communicated (e.g. risk expectations, acquisition standards, and technological direction).3. Departmental IT plans are linked to departmental strategic plans and government-wide initiatives (e.g. shared services) and include both short-term and long-term time frames.
Processes are in place for planning the acquisition of IT assets.	<ol style="list-style-type: none">1. Plans for the acquisition of assets are ranked and linked to the overall IT plan.2. Plans for IT asset acquisitions take into consideration life cycles and risk.3. Plans for IT asset acquisitions are consolidated internally for configuration and cost considerations.4. Plans for IT asset acquisitions take into consideration shared services through common service providers and with other departments.
Processes are in place for monitoring the performance of IT assets.	<ol style="list-style-type: none">1. Asset performance is monitored, including financial and non-financial key performance indicators for purchasing and maintenance.2. Asset tracking systems are in place for inventory management, including software licences.

Appendix B: Departments and Agencies Included in the Audit Engagement

Small Departments and Agencies

1. Canada Industrial Relations Board
2. Canadian Centre for Occupational Health and Safety
3. Canadian Intergovernmental Conference Secretariat
4. Farm Products Council of Canada
5. National Film Board of Canada
6. Office of the Commissioner for Federal Judicial Affairs Canada
7. Office of the Communications Security Establishment Commissioner
8. Patented Medicine Prices Review Board Canada
9. Public Servants Disclosure Protection Tribunal Canada
10. Public Service Labour Relations Board
11. Registry of the Specific Claims Tribunal of Canada

Central Agency

1. Treasury Board of Canada Secretariat

Common Service Provider included in the audit for the purpose of

1. Public Works and Government Services Canada

Appendix C: Ranking of Recommendations

The following table presents the recommendations and their assigned priority ranking. Rankings were determined based on the relative importance of the recommendations across the government and their potential to motivate long-term change and reduce risk across the government.

Recommendations	Priority
1. TBS, in collaboration with SDAs, should determine whether government wide IT policies governing the management of IT in SDAs are consistent with the IT management risks of SDAs.	High
2. SDAs should ensure their IT plans for proposed acquisitions address areas of highest priority in terms of risk, life cycle of assets, or operational needs.	Medium
3. TBS should identify and resolve the barriers that limit the adoption of shared IT assets and services by SDAs where appropriate. This activity should include an examination of parallel infrastructures that present an opportunity for rationalization or sharing.	High
4. SDAs should develop processes for measuring the performance of IT to ensure that they have objective information to support their management decisions about IT.	Medium
5. TBS should ensure that the performance indicators that have been developed for IT have been communicated appropriately to those who are responsible for collecting data and measuring performance.	Medium

Appendix D: Links to Applicable Frameworks, Policies, and Directives

Frameworks, Policies, and Directives

[Policy Framework for Information and Technology](#)

[Policy on Management of Information Technology](#)

[Directive on Management of Information Technology](#)

[Policy Framework for the Management of Assets and Acquired Services](#)

[Policy for Investment Planning – Assets and Acquired Services](#)

[Control Objectives for Information and related Technology – CobiT](#)

[1]. The Office of the Comptroller General has not undergone an external assessment at least once in the past five years or been subject to ongoing monitoring or to periodic internal assessments of its horizontal internal audit activity that would confirm its compliance with these standards.