Final Report

2007-722

Audit of the Configuration Management Processes Across PWGSC

Office of Audit and Evaluation

March 19, 2009

Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada

Canada

Public Works and Government Services Canada
Audit and Evaluation Branch

2007-12-10

TABLE OF CONTENTS

MAIN POINTS

What was examined

i. Configuration Management (CM) is the detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components. Such information typically includes the software versions and updates that have been applied to installed systems, and the locations and network addresses of hardware devices. The purpose of CM is to identify all significant components within the infrastructure; to collect and manage details about these components; and to provide reliable and up-to-date information to other Information Technology (IT) areas.

ii. Central to CM is a Configuration Management Database (CMDB) which houses and tracks relevant IT components, versions, status and the relationships between them. These IT components are referred to as Configuration Items (CI). CIs can include hardware, software licenses, network components, servers, documentation, procedures, service level agreements, etc. The implementations of a CMDB within an enterprise can include a single database solution (typically referred to as a Corporate Configuration Database or CCMDB) or a series of integrated CMDBs called a Federated Configuration Management Database or FCMDB.

iii. Configuration Management is related to IT Asset Management. IT Asset Management maintains details on IT assets such as hardware and software and their locations. Configuration Management also maintains relationships between IT assets, which IT Asset Management usually does not.

Why it is important

iv. Strong configuration management processes support the proper management and control of the department’s IT infrastructure. Without reliable configuration management information, impacts to critical systems may not be identified in a timely manner, which may ultimately result in system failures and in delays in recovering from these failures.

v. The Configuration Management Process supports other key Information Technology Infrastructure Library (ITIL) processes, such as Change Management, Availability Management, and Security Management. In this regard, it is important to have configuration management in place to facilitate the recovery of systems in the case of failure. Configuration Management assists the department in identifying characteristics of its hardware and software. This knowledge is necessary to assist the department in determining which hardware or software needs to be upgraded for performance and security reasons.

What was found

vi. Public Works and Government Services Canada (PWGSC) has several Configuration Management repositories, however they do not identify PWGSC critical systems. While PWGSC has identified its critical services, it has not mapped those critical services to the critical applications supporting them. Additionally, critical applications have not been mapped to critical components of the IT infrastructure. Given the above, it is not known if priority would be allocated to appropriate systems in the case of a Disaster Recovery circumstance.

vii. The existing configuration management processes within PWGSC are inconsistent across the organization for the systems audited. There are many repositories (configuration management databases, spreadsheets, small applications) used by various infrastructure groups and organizations within PWGSC. There is little communication or synergies across these repositories and organizations. Data stored within these repositories varies in quality, completeness and accuracy.

viii. In April 2006, the Information Technology Services Branch (ITSB) initiated the Corporate Configuration Management Database (CCMDB) pilot project. The goal of this project was to create a central repository to store information regarding all relevant IT components, for all infrastructure groups and stakeholders. As of June 2008, the database had been implemented and the plan is to keep it operational, however further advancements are not expected as the CCMDB development project was archived due to lack of funding. The CCMDB and other existing PWGSC systems only meet a portion of PWGSC's needs.

Recommendations and Management Action Plan

Management Response

Information Technology Services Branch considers that the results of the Audit accurately and fairly reflect the state of the Configuration Management Processes in the areas audited. The Information Technology Services Branch intends to act on the recommendations of the audit by implementing a Management Action Plan, detailed as follows.

The Chief Executive Officer Information Technology Services Branch should:

1. Establish a consistent configuration management process, which provides reliable and up-to-date information. The configuration management process should be integrated with the other Information Technology Infrastructure Library processes, and with Security Management. The process should include the identification of roles and responsibilities, support the identification of critical

systems, and provide information in support of recovery of a system in case of a failure.

Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

1.1 The implementation of the Information Technology Infrastructure Library (ITIL) by the Information Technology Services Branch (ITSB) is an on-going process. The current configuration management process will be updated to ensure that it supports the identification of critical systems and provides information in support of recovery of those critical systems in case of a failure. This action will be completed by June 30th, 2009.
1.2 ITSB will develop a high level roadmap, an end-to-end implementation plan, integrated with the ITIL processes, and with Security Management, including a high level assessment of the funding required to address the recommendation in full. This action will be completed by May 29th, 2009.
1.3 ITSB will prepare and present a business case to the Chief Financial Officer to obtain departmental approval for the most appropriate and cost-effective approach towards the implementation of a configuration management process. This action will be completed by July 31st, 2009.
1.4 If the funding identified in the business case is refused in whole or in part, ITSB will inform the appropriate departmental committee of the impact of the decision. In the absence of funding, the configuration management process may not be fully integrated with ITIL, but ITSB will ensure that the process will include the identification of roles and responsibilities, will support the identification of critical systems, and will provide information in support of recovery of those systems in case of simple or catastrophic failure. This action will be completed by March 31st, 2010. A configuration management process, which is not fully integrated with the other ITIL processes, and with Security Management, reduces the ability of PWGSC to manage its IT Services more efficiently. This risk will be reduced as ITSB continues to implement ITIL over time.
1.5 Assuming the approval of the business case presented in 1.3 above, ITSB will fully implement a consistent configuration management process fully integrated with other ITIL disciplines for its current and operational infrastructure components, by September 30th, 2010.
1.6 Assuming the approval of the business case presented in 1.3 above, ITSB will fully implement a comprehensive and consistent configuration management process for all operational applications, by September 30th, 2010.

2. Establish a repository or several repositories that meets the configuration management needs of the entire department.

Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

2.1 ITSB will continue to incrementally expand and improve its current configuration management processes reflected in its MS SQL-based Corporate Configuration Management Database (CCMDB) where the information currently defines the configurations of its mainframes and mid-range processors. The CCMDB will be updated to address the configuration management needs of the following infrastructure areas: Networks, Storage and Office Automation & Mail. Configuration management data related to these infrastructure areas will be migrated to the CCMDB. ITSB will ensure that all critical IT systems are tracked in one or more repositories. These activities will be completed by November 30th, 2009.

2.2 To meet the configuration management needs of the entire department, ITSB will prepare a business case to conduct a comprehensive study designed to meet the configuration management needs of the entire department. This action will be completed by November 30th, 2009.

2.3 ITSB will then prepare and present a business case to the appropriate executive body for funding and approval to proceed with the agreed direction, timeframes and funding. This business case will seek departmental approval to proceed with a "departmental" configuration management process to meet the configuration management needs of the entire department and to obtain the necessary funds. The residual risks associated with the various options presented in the business case will be clearly identified in that document. This action will be completed by February 28th, 2010

2.4 As directed by departmental decision, ITSB will establish repository or several linked repositories that meets the configuration management needs of the entire department, commensurate with the approved funding. This action will be completed by September 30th, 2010.

2.5 If the funding identified in the business case is refused in whole or in part, ITSB will inform the appropriate departmental committees of the impact of the decision. ITSB will report the status of residual risks to the Departmental IM/IT Steering Committee on a periodic basis. These actions will be completed by September 30th, 2010.

3. Seek department-wide buy in for a standardized approach to software license management and IT asset management and ensure that all software licenses are tracked.

Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

3.1 Via the presentation of a deck to the appropriate governance committee, the Chief Executive Officer (CEO) of ITSB will seek a departmental wide buy-in

for a standardized approach to software license management and tracking and IT asset management, including an identification of the required modifications or creation of new policy and governance instruments in support of a standardized approach to software license and IT asset management[1]. This activity will be completed by May 30th, 2009.

3.2 ITSB will prepare and submit a comprehensive business case to the Chief Financial Officer (CFO) by July 30th, 2009, seeking through the governance process

- 3.2.1 the approval to proceed with a centralized hardware, license management and tracking system(s) to enable IT asset management. This would include the governance framework, the budget allocation transfer and the high level administrative processes;
- 3.2.2 the required funding to be earmarked for the purchase of hardware, software, and related tools enabling software license management and tracking and IT asset management;
- 3.2.3 the approval to proceed while leveraging the on-going investment in the ITAM[2] (Information Technology Asset Management) – a cradle to grave asset management system with the IT assets defined in note 1 to be within the scope of ITAM.

3.3 In the event the business case is not approved, ITSB will implement ITAM in a decentralized environment while maintaining a rigid regime for the management of its IT hardware and software assets identified in note 1. A decentralized environment means that phases of the asset life cycle management will continue to reside outside of ITSB and ITSB will only manage those assets under its control. The risk will remain that PWGSC, and not ITSB, may underutilize some of the software licenses procured. Milestones are described in note 2.

3.4 Following the approval to proceed by the departmental governance process, ITSB will prepare, seek approval and publish the required policy instruments, along with supporting standards and directives aimed at implementing this recommendation at the departmental level. This action will be completed by March 30th 2010.

3.5 Following the approval to proceed by the departmental governance process, ITSB will implement a comprehensive IT asset management process for all PWGSC IT assets as directed by the departmental governance process. This action will be completed by September 30th, 2010.

Note 1: Hardware and Software Assets within the Scope of the Information Technology Asset Management (ITAM).

[1] For a description of what components are in scope for ITAM, see note 1 – Hardware and Software Assets within the Scope of ITAM.
[2] For a description of the Information Technology Asset Management project, see note 2

Infrastructure	Servers, Firewalls, Routers / Gateways, Storage Array Networks (SAN), Mainframes, Uninterrupted Power Supply (UPS) Devices, Generators, Switches, Load Balancers (not a complete listing)
Print Devices	Printers, Print Servers
Wireless	Blackberry, Cell Phone, Pager
Workstation	Network Connected Desktop, Monitor, Laptop
Software	Commercial Off-the-Shelf (COTS) Software (including licenses)

Note 2: ITAM Definition:

ITAM is the management of PWGSC's IT assets from cradle to grave, or in ITAM lifecycle terms, from the initial request to purchase the IT asset, to its eventual disposal. The ITAM function includes the development and maintenance of policies, standards, processes, systems and measurements that enable AMCC (Asset Management Competency Center), on behalf of PWGSC, to manage PWGSC's IT asset portfolio with respect to risk, cost, control, IT governance, compliance and business performance objectives. ITAM is a process-driven approach that updates an ITAM repository to reflect changes to an IT asset resulting from any process activity throughout an IT asset's lifecycle. The ITAM repository plays a crucial role in providing various ITAM stakeholders with information to make both tactical and strategic decisions related to the delivery of IT services.

Phase 1 established a single ITAM repository for ITSB IT Asset Reporting, the implementation of an ITAM Discovery toolset and operationalization of a Reconciliation Team (January 2007 to March 2007 – Completed).
Phase 2 established the single ITAM repository for PWGSC IT Asset Reporting, monthly IT Asset reports and new/enhanced processes and procedures for keeping the ITAM Repository current (April 2007 to September 2007 Completed).
Phase 3 focused on the enhancement of processes and procedures that further increased ITAM data accuracy and reduced manual effort (October 2007 to March 2008 Completed).

ITAM Project Phases 4 & 5 will support the implementation of the following three key deliverables (April 2008 to March 2009 In Progress):
1. A PWGSC Software Asset Management Program;
2. An ITAM Reporting Dashboard; and
3. Formalized processes and procedures for hardware and software assets: receiving, evergreening, change management and disposal, which further enhance

the ITAM Program's embodiment of best practices by ensuring maximum coverage by ITAM of an IT Asset's lifecycle activity.

ITSB is moving towards a Phase 6. The planning for this phase is still in progress but it is the intention that this will encompass an end-to-end ITAM implementation for PWGSC.

4. Examine the feasibility of limiting administration rights of users on Personal Computers where possible.

   Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

   4.1 ITSB will perform a study to examine the feasibility of limiting the administration rights of user of personal computers and including the identification of the most appropriate funding avenue. This activity will be completed by November 30th, 2009.
   4.2 Based on the recommendations of the study, ITSB will limit administration rights of users on Personal Computers. This activity will be completed by March 30th, 2010.

5. Ensure that the Information Technology Shared Services Certification Authority monitors all Interim Authority to Operate for the Information Technology Shared Services Infrastructure.

   Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following action:

   5.1 ITSB will formalize the role of the IT Shared Services (ITSS) Certification Authority (CA) and will develop and implement processes to ensure that all Interim Authority to Operate (IAOs) are accurately monitored. This activity will be completed by November 30th, 2009.

Management Response

The Assistant Deputy Minister of Corporate Services, Policy and Communications Branch accepts the recommendation that Corporate Services, Policy and Communications

Branch ensures that a mapping of critical services to critical applications and critical applications to critical infrastructure is performed in support of Public Works and Government Services Canada critical systems. Following is the Management Action Plan for Corporate Services, Policy and Communications Branch's deliverable in response to this audit.

The Assistant Deputy Minister of Corporate Services, Policy and Communications Branch should:

1. Ensure that a mapping of critical services to critical applications, and critical applications to critical infrastructure, is performed in support of the identification of PWGSC critical systems.

   Corporate Services, Policy and Communications Branch's response. Corporate Services, Policy and Communications Branch accepts the recommendation and will be taking the following actions:

   1.1 Phase I: Identification of critical services and completion of Business Impact Analyses, including the mapping of IT requirements. There are 23 formal steps in this process. For the purposes of this action plan, they are summarized as follows:
   - 1.1.1 Hold kick-off meetings and briefings
   - 1.1.2 Provide training
   - 1.1.3 Update and revise Business Impact Analyses
   - 1.1.4 Vet the Business Impact Analyses
   - 1.1.5 Conduct IT Requirements Map Workshop
   - 1.1.6 Formal sign off and approval of Business Impact Analyses.

   Phase I will be conducted in two waves. The first wave involves: Accounting, Banking and Compensation Branch (ABCB), Acquisitions Branch (AB), Translation Bureau (TB), Human Resources Branch (HRB), Real Property Branch (RPB) and Information Technology Services Branch (ITSB). Wave Two involves all other Branches, the Regions, and Audit Services Canada. Phase I, Wave One is complete. Phase I, Wave Two began in January 2009 and is targeted for completion in April 2009.

   1.2 Phase II: Identification of linkages between applications and IT infrastructure. This phase will also be divided into two Waves, using the same breakdown as in Phase I. Wave One: ABCB, AB, TB, HRB, RPB and ITSB. Wave Two: All other Branches, the Regions, and Audit Services Canada. Phase II, Wave One began in January 2009 with targeted completion date of March 2009. Phase II, Wave Two is targeted for completion in July 2009.

INTRODUCTION

1. Public Works and Government Services Canada's (PWGSC) Information Technology Services Branch (ITSB) is the organizational unit responsible for the management of both PWGSC and select government-wide computing services and assets. The responsibilities of the Service Management and Delivery Sector within ITSB include the additions, changes, replacements and maintenance of system configurations for all systems operating within PWGSC's environment – PWGSC owned or otherwise.

2. In order to manage Information Technology (IT) support more efficiently and effectively and to improve on the quality of service delivery provided to internal and external clients, ITSB is progressively moving towards an IT Infrastructure Library (ITIL) framework for service management and delivery. ITIL is an industry best practice for IT Service Management. Its aim is to effectively manage customer requirements, quality and costs through the competent management of IT services. Activities are divided into processes which, when used together, help optimize the level of support and delivery achieved by PWGSC. One such process is Configuration Management. Configuration Management supports the other nine ITIL processes, as well as Security Management. The other nine ITIL processes are: Incident Management, Problem Management, Change Management, Release Management, Service Level Management, Financial Management for IT Assets, Capacity Management, IT Service Continuity Management, and Availability Management.

3. The basic activities of Configuration Management are as follows: Planning - planning and defining the purpose, scope, objectives, policies and procedures for Configuration Management; Identification - selecting and identifying the configuration structures and items within the scope of the IT infrastructure (this includes owners, attributes, dependencies and relationships between configuration items); Configuration Control - ensuring that only authorized and identifiable configuration items are accepted and recorded in the CMDB throughout its lifecycle; Status Accounting - keeping track of the status of components throughout the entire lifecycle of configuration items e.g. from 'In Production' to 'off-line' and 'retired', and; Verification and Audit – reviewing and auditing after the implementation of configuration management to verify that the correct information is recorded in the CMDB.

4. Configuration Management is related to IT Asset Management. IT Asset Management (ITAM) maintains details on IT assets such as hardware and software and their locations. Configuration Management also maintains relationships between IT assets, which IT Asset Management usually does not.

5. Three systems were included as part of this audit, namely the ITAM System, the Mid Range Information System (MRIS), and the Corporate Configuration Management Database (CCMDB). The ITAM system is used by ITSB to manage some of PWGSC's IT assets, from the initial purchase request to its eventual disposal. It is important for an ITAM System to provide information to a Configuration

Management Database (CMDB), as this allows PWGSC to better manage its services that depend on those IT assets. MRIS contains the largest centralized collection of Configuration Items (CIs) within PWGSC. Finally, the CCMDB was chosen because it was to address the configuration needs of five infrastructure areas (Mid Range, Mainframe, Networks, Storage and Office Automation & Mail) within one repository.

6. In April 2006 a pilot project was initiated to create one CCMDB. This CMDB was initially referred to as the Federated CMDB, and was subsequently referred to as the CCMDB. The benefits of the project include maintenance cost reductions; up to date, accurate and timely information about assets and associations (including legal and contractual obligations); and a reduction in the risk of unplanned changes to the IT Infrastructure. A decision to stop the funding for the CCMDB project was made in June 2008. While the CCMDB database had been implemented and is intended to remain operational, the project is currently being archived and no additional work or project development will be performed in this area with exception of adding CIs from the storage group.

FOCUS OF THE AUDIT

7. The objective of this internal audit was to assess the effectiveness and efficiency of the existing configuration management processes at PWGSC.

8. The three systems included in the scope of the audit are the: IT Asset Management System, the Mid Range Information System, and the Corporate Configuration Management Database.

9. More information on the objective, scope and approach, and criteria can be found in ‘About the Audit’ section at the end of the report.

OBSERVATIONS

A Configuration Management Solution that meets the needs of PWGSC has not been established

10. A Configuration Management Solution for an organization the size of PWGSC requires the use of one or more CMDBs. A CMDB is a repository which houses and tracks relevant IT components, versions, status and the relationships between them. A solution that meets the needs of PWGSC is important to manage the IT Infrastructure effectively. For instance, such a solution would enable PWGSC to ensure that any change made to one system does not adversely affect any of the other systems. It would also enable PWGSC to better manage its critical systems. We expected evidence of the use of either a CCMDB or a Federated Configuration Management database (FCMDB) which meets the needs of PWGSC.

11. We found that:

    - No single CMDB or multiple integrated CMDBs exists within PWGSC to service all of PWGSC.

    - ITSB has implemented a Corporate CMDB, however not all groups within ITSB that practice Configuration Management are using it. A number of groups use spreadsheets as a Configuration Management Repository.

    - One group within the Information Technology Services Branch (ITSB) has not fully addressed its Configuration Management needs.

12. PWGSC does not have a configuration management solution that meets all of its needs. This reduces the ability of PWGSC to manage its IT Services more efficiently.

Consistent configuration procedures have not been established to support management and recording of changes to the configuration repository

13. Configuration procedures specify how personnel create and maintain the information in the configuration management repositories. Consistency within configuration procedures ensures data integrity, data accuracy and reduces reporting challenges. We expected consistent configuration procedures to support management and recording of changes to the configuration repository.

14. We found that the CCMDB has some procedures defined to support the management and recording of changes to the Configuration Items. There are some infrastructure areas within ITSB that use their own repositories with varying procedures instead of the CCMDB. As well, the information in the CCMDB is incomplete and in some cases inaccurate.

15. As a result, PWGSC does not have a complete and integrated view of a baseline of configuration items maintained for its systems and services. This limits the quality and the completeness of the information that Configuration Management can provide to the other nine ITIL processes, thus reducing the ability of PWGSC to manage its IT Services in the most efficient manner.

Configuration Management process is minimally integrated with the other ITIL processes, and Security Management

16. Individual processes often are combined to perform an action and as a result, processes need to be integrated. Integrated ITIL processes increase the efficiency of the IT Service Provider. We expected that the configuration management process would be integrated with the other nine ITIL processes, and Security Management.

17. We found that:

    - The Configuration Management process used for the CCMDB is minimally integrated with the other nine ITIL processes and with Security Management.

18. The lack of integration between the Configuration Management process and the other ITIL processes and with Security Management reduces the ability of PWGSC to manage its IT Services in the most efficient manner.

Periodic review of the configuration data in the CCMDB does not occur to verify and confirm the integrity of the current and historical configuration

19. Periodic reviews help to ensure data integrity and data completeness of Configuration Items, which in turn allows PWGSC to return all of its systems back to a known and stable state in the instance of an adverse effect caused by a change to its systems. In addition, it allows Configuration Management to properly support all the other ITIL processes. We expected that evidence of periodic reviews of the configuration data occurs to verify and confirm the integrity of the current and historical configuration.

20. We found that procedures for the CCMDB do not include periodic reviews of the configuration data. The unwritten policy is “if you touch it, you review and update it”. Some data contained within the CCMDB is inaccurate and incomplete.

21. The inaccurate and incomplete data in the CCMDB reduces the ability of PWGSC to manage its IT Services more efficiently.

Scope of CCMDB project and system was poorly communicated

22. The scope of a project addresses requirements, budget, and timelines. It is important to communicate the scope of a project to those who will use it or need to interface to it, so that they can plan ahead. We expected that the scope of the CCMDB project and system would have been clearly communicated to stakeholders to ensure their participation and support.

23. We found that the CCMDB project and system were poorly communicated to stakeholders such as Configuration Item (CI) Owners and other ITIL process owners. The Service Categorization Framework used by ITSB has services defined into three layers: Operational Management Layer; Product / Service Layer; and the Client Facing Layer. The scope of the CCMDB project was limited to the Operational Management Layer. This scope limitation was not clearly communicated to stakeholders.

24. The CCMDB is a pilot project based on technology not considered to be an enterprise class solution and therefore may not be capable of handling the volumes required to meet the needs of the entire department. Project documentation (including the project

charter) and communications (CCMDB presentations) did not clearly specify the limitations of the selected CCMDB platform. Furthermore, there was no marketing plan for the CCMDB to ensure that all stakeholders embraced the new system.

25. The lack of communication regarding the scope of the CCMDB project and system led to lost opportunity within ITSB to maximize its use of the CCMDB and to address its limitations as early as possible.

There is no role responsible for centralized monitoring of Configuration Items and for ensuring that CI Owners follow consistent Configuration Management processes

26. CI's form the basis of configuration management. They typically include items such as hardware, software, and formal documentation. A configuration item owner has primary responsibility for a configuration item. Without accurate and complete information, the quality of support that Configuration Management provides to the other ITIL processes is affected and may lead to erroneous decisions, costly errors and security breaches.

27. We expected that there would be clear roles and responsibilities, including a role for centralized monitoring of Configuration Items and for ensuring that CI Owners follow consistent Configuration Management processes. This is required to ensure that CIs are accurate and complete.

28. We found that there is no defined role for centralized monitoring of Configuration Items and for ensuring that CI Owners follow consistent Configuration Management processes. Data was found to be inconsistent and incomplete. As a result, the inaccurate and incomplete data in the CCMDB reduces the ability of PWGSC to manage its IT Services in the most efficient manner.

Not all PWGSC IT assets are recorded in the IT Asset Management System

29. IT assets includes all the hardware and software items including PCs, servers, network devices, accessories, software licenses, updates, and in-house developed software. An enterprise needs to know what IT assets it has to manage them throughout their lifecycle, to identify underutilized hardware and software, to reduce inventories, and to better manage the services supported by the IT assets. We expected that all relevant PWGSC IT assets and changes to assets were recorded in the IT Asset Management System.

30. We found that the project to implement a department-wide IT Asset Management (ITAM) tool was partially completed. New servers, most Personal Computers (PC) and other devices were included within the system. However some PCs, software and some classes of devices such as cell phones and BlackBerries were not yet tracked using the tool. Although the Department uses tools to monitor devices attached to the network, not all devices are accessible to the tools as they are hidden behind firewalls.

Finally, some IT devices, including some PCs, are purchased without the involvement of ITSB and are not included in the ITAM system.

31. As a result, PWGSC is not positioned to manage its IT Assets and the services that depend on these assets in the most effective manner.

Critical systems within PWGSC have not been identified

32. The Government of Canada Security Policy states "Departments must identify and categorize assets, especially critical services, based on the degree of injury (low, medium, high) that could reasonably be expected to result from compromise to their availability or integrity". The Policy defines a critical service as a "service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well being of Canadians, or to the efficient functioning of the Government of Canada". To support these critical services, the business applications and infrastructure supporting these critical services, also known as critical systems, must be known and documented. This requires that critical services be identified and mapped to supporting critical applications; and those critical applications be mapped to critical components of the IT infrastructure. Configuration Items contained within the Configuration Management Database related to critical services should be identified as such. A full mapping of critical services to the IT infrastructure allows PWGSC to plan for recovery of critical systems in a timely manner.

33. We expected that PWGSC would have the necessary information within its CMDBs to identify its critical systems and critical configuration items that make up those critical systems.

34. A recommendation in the *2003-726 Audit of IT Infrastructure Component (BCPs) of the Corporate Business Continuity Plans* reads "Linkages between the list of Critical Services, business units, and the IT Infrastructure components of BCPs required to ensure availability, needs to be established, and a risk management process be included for prioritization of these services".

35. We found that:

- A list of ten critical services for PWGSC is in place and a project is currently underway, led by the Corporate Emergency Preparedness group within Corporate Services, to map these critical services to applications and IT infrastructure.

- ITSB has established a list of critical systems that predates the 2003-726 Audit.

36. We concluded that although PWGSC has identified its critical services, PWGSC has not identified its critical systems. As a result, there is a risk that PWGSC contingency plans may be incomplete which may lead to PWGSC being unable to deliver critical

services in case of supporting critical system failure. We understand that recently there has been a renewed effort on the part of PWGSC to identify its critical systems.

A department-wide framework for the tracking and controlling of software licenses has not been defined.

37. A software license is a legal instrument governing the usage or redistribution of copyright protected software. Without a proper license tracking and controlling framework, PWGSC may underutilize the software licences it has procured for some products, and it may not be able to detect potential software licence infringements. We expected that effective and consistent processes for the monitoring and management of desktop and server software licenses would exist.

38. The process for managing software licenses was reviewed in two branches: Consulting, Information and Shared Services Branch (CISSB) and Real Property Branch (RPB). We found that there is no formal process or policy in place governing software license management at the departmental level and several tools are in place but there is no coordinated toolset used in the overall determination of inventory. As a result, there is inconsistent control over software licenses. These two Branches are managing the process in different ways, ranging from spreadsheets to small applications. Quality and control over license management is largely dependent on the client authorities assigned to the branch.

39. We determined that Real Property Branch had strong management over software licenses, and possessed good toolsets to track and monitor usage. CISSB recently took over license management for Audit Services Canada and Government Consulting Services and discovered they had installed licenses of two software products on significantly more computers than the number of licenses purchased. Consulting, Information and Shared Services Branch (CISSB) has since taken steps towards resolving this issue.

40. Current plans are for software license management throughout PWGSC to be eventually captured within Information Technology Asset Management (ITAM) and is scheduled for implementation in April 2009. However, there is currently no definitive framework or policy in place to help the branches determine optimum ways to manage software licences. As of July 2008, the ITAM group had not contacted branches across PWGSC to build upon good practices or to leverage existing tools.

41. Because there is no formal departmental framework for managing software licences, the quality of the information gathered is inconsistent. As a result there is a risk that PWGSC underutilizes the software licences it has procured for some products, and PWGSC may not be able to detect potential software licence infringements.

Configuration of personal computers gives the user administrative rights

42. Administrative rights allow a person to install, modify or delete software programs on their Personal Computers (PC). Without restricting administrative rights, PWGSC is restricting its capability to effectively manage software installations and maintain thorough control of software licenses. Controlling administrator rights can prevent unauthorized installation of software. We expected to that find PC configurations would be completed without the user having administrative rights where feasible.

43. We found that:

- Administrative rights are given to users on PWGSC PCs. This means that configuration cannot be controlled as users may install both authorized and unauthorized software. Without taking preventative measures including installation restrictions, the configuration management environment cannot be controlled.

- At present there is no communication between the ITAM system and the new CCMDB system. Communications between the ITAM system and the CCMDB system would facilitate the removal of administrative rights from users that do not require such rights.

44. There is a risk that anyone with administrative rights to their PCs may install unauthorized software, or that they may unknowingly allow unauthorized software to be installed on their PCs. This may lead to further risks to the integrity of the information that may be accessed through those PCs. While PWGSC already has measures in place to minimize such risks, such as the Department Policy 070 on the Use of Electronic Networks, and users are asked to accept on a periodic basis their responsibilities not to install unauthorized software, an examination of the feasibility of limiting administrative rights of users where feasible would provide PWGSC with the information it requires to determine whether this risk can be further mitigated.

There is no overall Interim Authority to Operate (IAO) monitoring system for IT Shared Services

45. The Government Security Policy (GSP) defines Certification as a comprehensive evaluation of the technical and non-technical security features of an IT system and other related safeguards to establish the extent to which a particular design and implementation meets a specific set of security requirements, made in support of the accreditation process. The GSP also defines accreditation as the official authorisation by management for the operation of an IT system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations. Without proper certification and accreditation, a system enters into production without meeting the standards of the Treasury Board and there is a risk of system failure, loss of critical data and data integrity issues.

46. An Interim Authority to Operate (IAO) is a temporary written approval to process sensitive information under a set of extenuating circumstances where the residual risk is not yet acceptable, but there is an operational necessity for the system under development. The conditions attached to the approval may require temporary safeguards to be put in place while the system is undergoing further design, development and testing. In some cases the Accreditation Authority will grant an Interim Authority to Operate (IAO) for a system to operate if a set of extenuating circumstances require that the system be "turned on" even though the risk is unacceptable. An IAO contains conditions, such as the type of information that can be processed and the expiry date of the IAO.

47. The monitoring of IAOs is an important control to assure senior management that the conditions attached to the approval of the IAO will be addressed in a timely manner and that a residual risk that is not yet acceptable will not be accepted for longer than it needs to by senior management. We expected that the CCMDB project team had renewed its IAO in a timely manner. We also expected that the CCMDB project team would be in the process of addressing or have addressed all high-risk items identified within the CCMDB Threat and Risk Assessment issued by the CCMDB project on April 25 2007.

48. We found that:

- The CCMDB IAO expired in October 2007.
- The Threat Risk Assessment dated April 25, 2007 determined that the current level of residual risk to the ITSB Corporate Configuration Management Database system is 'High'.
- Few steps had been taken to seek renewal/certification. Measures were recommenced to be taken in April 2008.
- The CCMDB project team determined the high risk ranked items identified within the TRA did not pertain to them. Rather, the project team thought the onus was on the ITSB Infrastructure group to action all items. There was a lack of coordination and communication between the two groups and as a result the issues were not addressed on a timely basis.
- The IT Shared Services Certification Authority does not monitor all IAOs related to the IT Shared Services Infrastructure.

49. The risks to the Corporate Configuration Management Database system have not been mitigated in a timely manner, as specified in the IAO conditions. Senior Management has *de facto* accepted a higher level of risk for a longer period than anticipated.

CONCLUSION

50. The existing configuration management processes within PWGSC are both inadequate and inconsistent across the organization for the systems audited. There are many Configuration Management repositories (configuration management databases, spreadsheets, small applications) used by various infrastructure groups and organizations within PWGSC. There is little communication amongst Configuration Management Stakeholders within ITSB and little synergies across ITSB configuration management repositories. Data stored within these repositories varies in quality, completeness and accuracy. Configuration Management processes require improvement to meet the needs of PWGSC. The current configuration management repositories in place do not meet the needs of PWGSC.

51. PWGSC has not identified its critical systems. As a result, there is a risk that PWGSC contingency plans may be incomplete which may lead to PWGSC being unable to deliver critical services in case of supporting critical system failure. A departmental-wide framework for the tracking of software licenses has not been defined. The IT Asset Management System does not currently track all relevant PWGSC IT assets. PWGSC users have administrative rights on their PCs, which creates a risk that they may unknowingly allow unauthorized software to be installed on their PCs.

RECOMMENDATIONS AND MANAGEMENT ACTION PLAN

Management Response

Information Technology Services Branch considers that the results of the Audit accurately and fairly reflect the state of the Configuration Management Processes in the areas audited. The Information Technology Services Branch intends to act on the recommendations of the audit by implementing a Management Action Plan, detailed as follows.

The Chief Executive Officer Information Technology Services Branch should:

1. Establish a consistent configuration management process, which provides reliable and up-to-date information. The configuration management process should be integrated with the other Information Technology Infrastructure Library processes, and with Security Management. The process should include the identification of roles and responsibilities, support the identification of critical systems, and provide information in support of recovery of a system in case of a failure.

Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

1.1 The implementation of the Information Technology Infrastructure Library (ITIL) by the Information Technology Services Branch (ITSB) is an on-going process. The current configuration management process will be updated to ensure that it supports the identification of critical systems and provides information in support of recovery of those critical systems in case of a failure. This action will be completed by June 30th, 2009.

1.2 ITSB will develop a high level roadmap, an end-to-end implementation plan, integrated with the ITIL processes, and with Security Management, including a high level assessment of the funding required to address the recommendation in full. This action will be completed by May 29th, 2009.

1.3 ITSB will prepare and present a business case to the Chief Financial Officer to obtain departmental approval for the most appropriate and cost-effective approach towards the implementation of a configuration management process. This action will be completed by July 31st, 2009.

1.4 If the funding identified in the business case is refused in whole or in part, ITSB will inform the appropriate departmental committee of the impact of the decision. In the absence of funding, the configuration management process may not be fully integrated with ITIL, but ITSB will ensure that the process will include the identification of roles and responsibilities, will support the identification of critical systems, and will provide information in support of recovery of those systems in case of simple or catastrophic failure. This action will be completed by March 31st, 2010. A configuration management process, which is not fully integrated with the other ITIL processes, and with Security Management, reduces the ability of PWGSC to manage its IT Services more efficiently. This risk will be reduced as ITSB continues to implement ITIL over time.

1.5 Assuming the approval of the business case presented in 1.3 above, ITSB will fully implement a consistent configuration management process fully integrated with other ITIL disciplines for its current and operational infrastructure components, by September 30th, 2010.

1.6 Assuming the approval of the business case presented in 1.3 above, ITSB will fully implement a comprehensive and consistent configuration management process for all operational applications, by September 30th, 2010.

2. Establish a repository or several repositories that meets the configuration management needs of the entire department.

Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

2.1 ITSB will continue to incrementally expand and improve its current configuration management processes reflected in its MS SQL-based Corporate Configuration Management Database (CCMDB) where the information currently defines the configurations of its mainframes and mid-range processors. The CCMDB will be updated to address the configuration management needs of the following infrastructure areas: Networks, Storage and Office Automation & Mail. Configuration management data related to these infrastructure areas will be migrated to the CCMDB. ITSB will ensure that all critical IT systems are tracked in one or more repositories. These activities will be completed by November 30th, 2009.

2.2 To meet the configuration management needs of the entire department, ITSB will prepare a business case to conduct a comprehensive study designed to meet the configuration management needs of the entire department. This action will be completed by November 30th, 2009.

2.3 ITSB will then prepare and present a business case to the appropriate executive body for funding and approval to proceed with the agreed direction, timeframes and funding. This business case will seek departmental approval to proceed with a "departmental" configuration management process to meet the configuration management needs of the entire department and to obtain the necessary funds. The residual risks associated with the various options presented in the business case will be clearly identified in that document. This action will be completed by February 28th, 2010

2.4 As directed by departmental decision, ITSB will establish repository or several linked repositories that meets the configuration management needs of the entire department, commensurate with the approved funding. This action will be completed by September 30th, 2010.

2.5 If the funding identified in the business case is refused in whole or in part, ITSB will inform the appropriate departmental committees of the impact of the decision. ITSB will report the status of residual risks to the Departmental IM/IT Steering Committee on a periodic basis. These actions will be completed by September 30th, 2010.

3. Seeks department-wide buy in for a standardized approach to software license management and IT asset management and ensure that all software licenses are tracked.

Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

3.1 Via the presentation of a deck to the appropriate governance committee, the Chief Executive Officer (CEO) of ITSB will seek a departmental wide buy-in for a standardized approach to software license management and tracking and IT asset management, including an identification of the required modifications or creation of new policy and governance instruments in support of a

standardized approach to software license and IT asset management[1]. This activity will be completed by May 30th, 2009.

3.2 ITSB will prepare and submit a comprehensive business case to the Chief Financial Officer (CFO) by July 30th, 2009, seeking through the governance process

- 3.2.1 the approval to proceed with a centralized hardware, license management and tracking system(s) to enable IT asset management. This would include the governance framework, the budget allocation transfer and the high level administrative processes;
- 3.2.2 the required funding to be earmarked for the purchase of hardware, software, and related tools enabling software license management and tracking and IT asset management;
- 3.2.3 the approval to proceed while leveraging the on-going investment in the ITAM[2] (Information Technology Asset Management) – a cradle to grave asset management system with the IT assets defined in note 1 to be within the scope of ITAM.

3.3 In the event the business case is not approved, ITSB will implement ITAM in a decentralized environment while maintaining a rigid regime for the management of its IT hardware and software assets identified in note 1. A decentralized environment means that phases of the asset life cycle management will continue to reside outside of ITSB and ITSB will only manage those assets under its control. The risk will remain that PWGSC, and not ITSB, may underutilize some of the software licenses procured. Milestones are described in note 2.

3.4 Following the approval to proceed by the departmental governance process, ITSB will prepare, seek approval and publish the required policy instruments, along with supporting standards and directives aimed at implementing this recommendation at the departmental level. This action will be completed by March 30th 2010.

3.5 Following the approval to proceed by the departmental governance process, ITSB will implement a comprehensive IT asset management process for all PWGSC IT assets as directed by the departmental governance process. This action will be completed by September 30th, 2010.

Note 1: Hardware and Software Assets within the Scope of the Information Technology Asset Management (ITAM).

[1] For a description of what components are in scope for ITAM, see note 1 – Hardware and Software Assets within the Scope of ITAM.

[2] For a description of the Information Technology Asset Management project, see note 2

Infrastructure	Servers, Firewalls, Routers / Gateways, Storage Array Networks (SAN), Mainframes, Uninterrupted Power Supply (UPS) Devices, Generators, Switches, Load Balancers (not a complete listing)
Print Devices	Printers, Print Servers
Wireless	Blackberry, Cell Phone, Pager
Workstation	Network Connected Desktop, Monitor, Laptop
Software	Commercial Off-the-Shelf (COTS) Software (including licenses)

Note 2: ITAM Definition:

ITAM is the management of PWGSC's IT assets from cradle to grave, or in ITAM lifecycle terms, from the initial request to purchase the IT asset, to its eventual disposal. The ITAM function includes the development and maintenance of policies, standards, processes, systems and measurements that enable AMCC (Asset Management Competency Center), on behalf of PWGSC, to manage PWGSC's IT asset portfolio with respect to risk, cost, control, IT governance, compliance and business performance objectives. ITAM is a process-driven approach that updates an ITAM repository to reflect changes to an IT asset resulting from any process activity throughout an IT asset's lifecycle. The ITAM repository plays a crucial role in providing various ITAM stakeholders with information to make both tactical and strategic decisions related to the delivery of IT services.

Phase 1 established a single ITAM repository for ITSB IT Asset Reporting, the implementation of an ITAM Discovery toolset and operationalization of a Reconciliation Team (January 2007 to March 2007 – Completed).
Phase 2 established the single ITAM repository for PWGSC IT Asset Reporting, monthly IT Asset reports and new/enhanced processes and procedures for keeping the ITAM Repository current (April 2007 to September 2007 Completed).
Phase 3 focused on the enhancement of processes and procedures that further increased ITAM data accuracy and reduced manual effort (October 2007 to March 2008 Completed).

ITAM Project Phases 4 & 5 will support the implementation of the following three key deliverables (April 2008 to March 2009 In Progress):
1. A PWGSC Software Asset Management Program;
2. An ITAM Reporting Dashboard; and
3. Formalized processes and procedures for hardware and software assets: receiving, evergreening, change management and disposal, which further enhance

the ITAM Program's embodiment of best practices by ensuring maximum coverage by ITAM of an IT Asset's lifecycle activity.

ITSB is moving towards a Phase 6. The planning for this phase is still in progress but it is the intention that this will encompass an end-to-end ITAM implementation for PWGSC.

4. Examine the feasibility of limiting administration rights of users on Personal Computers where possible.

   Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following actions:

   4.1 ITSB will perform a study to examine the feasibility of limiting the administration rights of user of personal computers and including the identification of the most appropriate funding avenue. This activity will be completed by November 30th, 2009.
   4.2 Based on the recommendations of the study, ITSB will limit administration rights of users on Personal Computers. This activity will be completed by March 30th, 2010.

5. Ensure that the Information Technology Shared Services Certification Authority monitors all Interim Authority to Operate for the Information Technology Shared Services Infrastructure.

   Information Technology Services Branch's response. Information Technology Services Branch accepts the recommendation and will be taking the following action:

   5.1 ITSB will formalize the role of the IT Shared Services (ITSS) Certification Authority (CA) and will develop and implement processes to ensure that all Interim Authority to Operate (IAOs) are accurately monitored. This activity will be completed by November 30th, 2009.

Management Response

The Assistant Deputy Minister of Corporate Services, Policy and Communications Branch accepts the recommendation that Corporate Services, Policy and Communications Branch ensures that a mapping of critical services to critical applications and critical applications to critical infrastructure is performed in support of Public Works and Government Services Canada critical systems. Following is the Management Action Plan for Corporate Services, Policy and Communications Branch's deliverable in response to this audit.

The Assistant Deputy Minister of Corporate Services, Policy and Communications Branch should:

1. Ensure that a mapping of critical services to critical applications, and critical applications to critical infrastructure, is performed in support of the identification of PWGSC critical systems.

   Corporate Services, Policy and Communications Branch's response. Corporate Services, Policy and Communications Branch accepts the recommendation and will be taking the following actions:

   1.1 Phase I: Identification of critical services and completion of Business Impact Analyses, including the mapping of IT requirements. There are 23 formal steps in this process. For the purposes of this action plan, they are summarized as follows:
   - 1.1.1 Hold kick-off meetings and briefings
   - 1.1.2 Provide training
   - 1.1.3 Update and revise Business Impact Analyses
   - 1.1.4 Vet the Business Impact Analyses
   - 1.1.5 Conduct IT Requirements Map Workshop
   - 1.1.6 Formal sign off and approval of Business Impact Analyses.

   Phase I will be conducted in two waves. The first wave involves: Accounting, Banking and Compensation Branch (ABCB), Acquisitions Branch (AB), Translation Bureau (TB), Human Resources Branch (HRB), Real Property Branch (RPB) and Information Technology Services Branch (ITSB). Wave Two involves all other Branches, the Regions, and Audit Services Canada. Phase I, Wave One is complete. Phase I, Wave Two began in January 2009 and is targeted for completion April 2009.

   1.2 Phase II: Identification of linkages between applications and IT infrastructure. This phase will also be divided into two Waves, using the same breakdown as in Phase I. Wave One: ABCB, AB, TB, HRB, RPB and ITSB. Wave Two: All other Branches, the Regions, and Audit Services Canada. Phase II, Wave One began in January 2009 with targeted completion date of March 2009. Phase II, Wave Two is targeted for completion July 2009.

ABOUT THE AUDIT

Authority

The audit was approved by the department's Audit and Evaluation Committee as part of the 2008-2009 Internal Audit plan.

Objective

The objective of this internal audit was to assess the effectiveness and efficiency of the existing configuration management processes at PWGSC.

Scope and Approach

The audit examined and assessed the PWGSC configuration management environment including but not limited to the following:

1. Reviewed existing policies and procedures governing the PWGSC configuration management process.

2. Reviewed controls over the Configuration Management Database (CMDB) including the authorization process for adding, replacing and removing of Configuration Items.

3. Assessed the accuracy and validity of the Configuration Items within the CMDB environment through the selection and testing for the following three contribution systems: Mid Range Information System, IT Asset Management System and the new Corporate Configuration Management Database.

4. Verified the reliability of reporting and communication of Configuration Management information to/from other relevant ITIL processes, including Security Management.

Interviews were conducted with key personnel. Relevant processes and documentation were reviewed. Based on analysis of the information and evidence collected, the audit team prepared audit findings and conclusions, which were validated with the appropriate managers prior to tabling the Draft Final Report at the PWGSC Audit and Evaluation Committee.

The audit was conducted in accordance with the *Treasury Board Policy on Internal Audit* and the Government of Canada's Standards for Internal Auditing.

Criteria

Audit Criteria are the benchmarks or standards against which auditors compare their findings to develop audit observations and formulate conclusions. Suitable criteria must be relevant to the audit objective, complete, reliable, generally accepted, and understood by both the auditor and management.

The criteria for this audit are as follows:

1. A supporting tool and repository that contains relevant information on Configuration Items has been established.

2. IT Assets and changes to assets are recorded and monitored.

3. A baseline of configuration items is maintained for systems and services.

4. Configuration procedures have been established to support management and logging of changes to the configuration repository.

5. Configuration procedures are integrated with other relevant ITIL processes, including Security Management.

6. Periodic review of the configuration data occurs to verify and confirm the integrity of the current and historical configuration.

7. Periodic review of installed software against the policy for software usage occurs to identify personal or unlicensed software or any software instances in excess of current license agreements. Errors and deviations are reported, acted on, and corrected.

These criteria are derived from the IT Governance Institute, Control Objectives for Information and related Technology (COBIT® 4.1), the ITIL Framework and the Government Security Policy.

Audit Work Completed

The audit was conducted from January to July 2008 inclusive.

Audit Team

The audit team included one member of the Office of Audit and Evaluation supplemented by contracted personnel overseen by the Director, IT Audit and under the overall direction of the Chief Audit Executive, Office of the Audit and Evaluation.

The engagement was reviewed by the Quality Assessment function of the Office of Audit and Evaluation.