Health Canada Santé Canada

Final Audit Report

Audit of Data Integrity
MCCS Feeder System Interfacing with SAP

April 2008

Table of Contents

Executive Summary

The Management of Contracts and Contributions System (MCCS) was introduced in all regions of the Health Canada – First Nations Inuit Health Branch (FNIHB) in December 2001, with full implementation in April 2002. MCCS is an electronic system implemented nationally to enhance the Branch's ability to report, monitor, and audit its contracts and contribution agreements (CCA's). Health Canada's Framework for Integrated Resource Management System (FIRMS) uses SAP version R/3 for entering transactions, interfacing with various internal systems. MCCS is one of these feeder systems that provide data to SAP. MCCS processed approximately $827 million dollars of grant and contributions in Fiscal Year 2006-07.

The two objectives of the audit were to:

- determine the quality of the data, in terms of completeness and accuracy, of systems that interface with FIRMS/SAP; and
- provide an overall assessment of the internal control environment around MCCS.

The review was conducted by the Audit and Accountability Bureau in accordance with the Government of Canada's *Policy on Internal Audit*

Based on results from detailed testing of both MCCS and SAP, it was determined that the data being interfaced with SAP is accurate. The completeness of the data that is being interfaced with SAP could not be determined because MCCS does not generate control totals to compare input and output with SAP. This is a necessary control required to balance the data that is being interfaced from MCCS to SAP. There is a risk of not knowing if all of the data has been interfaced with SAP. At the time the audit was conducted, FNIHB was in the process of adding this functionality to MCCS. The general controls environment overall is operating satisfactorily, however, there needs to improved monitoring of super user access as well as improvements to the documentation regarding operating procedures.

Introduction

Background

The Management of Contracts and Contributions System (MCCS) was introduced in all regions of Health Canada – First Nations Inuit Health Branch (FNIHB) in December 2001, with full implementation in April 2002. MCCS is an electronic system implemented nationally to enhance the Branch's ability to report, monitor, and track information related to its contracts and contribution agreements (CCA's)

Health Canada's Framework for Integrated Resource Management System (FIRMS) uses SAP for entering transactions, interfacing with various internal systems such as the Management of Contributions & Contracts (MCCS). The data within SAP is used to generate financial and management reports which provide management with information to effectively manage the Department's financial resources.

The audit was undertaken by the Audit and Accountability Bureau in accordance with the Health Canada Risk-Based Audit Plan, for the period 2006-2007 to 2008-2009, which was approved by the Departmental Audit and Evaluation Committee on October 4, 2006. The audit was conducted in accordance with the Government of Canada's *Policy on Internal Audit*

Audit Objectives

The two objectives of this audit were to:

- determine the quality of the data, in terms of completeness and accuracy, of systems that interface with FIRMS/SAP; and
- provide an overall assessment of the internal control environment around MCCS.

The lines of enquiry for the audit included:

- automated field edits in the MCCS system;
- controls to ensure that all data was successfully interfaced;
- transaction controls;
- error processing;
- segregation of responsibilities;
- access controls; and
- problem management.

Scope and Approach

The scope of the audit focused on the integrity of data in MCCS which is interfaces with SAP. The audit also included an assessment of the internal control environment around MCCS. For the period April 1, 2005 to March 31, 2006, we have been able to identify the total value of all G&Cs interfaced from MCCS to FIRMS as approximately $827 million.

The audit of the MCCS interface was conducted in the National Capital Region. The audit consisted mainly of interviews with departmental officials of Health Canada, a review of relevant documentation and tests of the general computer controls and application controls associated with the MCCS to SAP interface. As the audit was conducted early in 2007, complete fiscal year 2006-2007 data did not exist. Accordingly, a decision was made to examine the interface files from January 1 to December 31, 2006.

Evidence gathered and analysed consisted of the actual data files transferred from MCCS to SAP during the calendar year 2006. Specific tests were conducted in the Ontario Region. The interface files were verified to the information reported in the actual Program/Finance files.

The project was conducted in accordance with the Government of Canada's *Policy on Internal Audit*. The audit was conducted using ISACA's COBIT (Control Objectives for Information and Related Technology) which is an IT governance model

A general controls review was conducted to gain an overall impression of the controls that are present in the MCCS environment. The application controls review included validation of various data inputs, logical access control and authorization and exception handling and logging.

Findings, Recommendations and Management Response

Completeness and Accuracy of Data

Output Balancing and Reconciliation

Procedures should exist to ensure output is routinely balanced to the relevant control totals. Audit trails should exist and facilitate the tracing of transaction processing and the reconciliation of disrupted data.

We attempted to select a sample of interface files to generate a control total for each file. We then attempted to verify the calculated control total with the actual SAP interface control total for the dates of the interfaces. This reconciliation could not be accomplished because neither the MCCS system nor the SAP system is programmed to generate any control totals for the interface.

Without control totals, management is at risk of not knowing whether all the information from MCCS was actually interfaced into SAP. However, the compensating control is that a recipient will likely notify the department if they have not received the correct payment within the appropriate time frame.

Recommendation No. 1

It is recommended that the Director General of Business Planning and Management Directorate (BPMD), First Nations Inuit Health Branch (FNIHB), develop a SAP/MCCS reconciliation process.

Management Response

Accept. Management is aware of this situation and is currently developing an automated SAP/MCCS reconciliation process. This has been implemented as of October 26, 2007.

General Controls Environment

Management Review of User Accounts

Management should have a control process in place to review and confirm access rights periodically. A periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorized alteration.

We found no policy enforcing formal standard operating procedures for Database Administrators (DBAs) and Super User access reviews:

- formal procedures for the management review of DBA and Operating System level Super User access is not available or documented; and
- 11 out of 17 user account change requests did not identify the reason for the change. Only the job function related to the user privilege was identified.

Since no policy for access review is documented, the department is exposed to the risk that certain access privileges that are no longer required, are still in effect with the potential for mis-use. Management is also at risk of not knowing the reason for granting access privileges or changing privileges.

Recommendation No. 2

It is recommended that the Director General of Business Planning and Management Directorate (BPMD), First Nations Inuit Health Branch (FNIHB):

a) request that the Chief Information Officer (CIO) establish and document standard operating procedures for monitoring the activities of the MCCS DBA and Super Users with access to the operating system; and

b) ensure that the MCCS User Access Request Form is enhanced to capture the reason for modifying privileges on an existing MCCS account.

Management Response

a) Accept. The Director General, BPMD has consulted the CIO of Health Canada who will provide standard operating procedures for monitoring the activities of the MCCS DBA and Super Users.

b) Accept. The MCCS account request form will be enhanced to capture the reason for privilege modification.

User Access Rights

User access rights to systems should be centrally managed and based on defined and documented business needs and job requirements. User access rights are requested/approved by user management and implemented by MCCS account administrator (and partially by a Health Canada Novell LAN administrator). Procedures should also exist to ensure that only authorized staff members perform data input.

User access rights to the MCCS system are centrally managed by the MCCS Support Team of Business Planning and Management Directorate (BPMD) of FNIHB. User access rights are based on defined and documented business needs, job requirements. They are requested/approved by user management and implemented by the MCCS Support Team. Every six months the MCCS Support Team produces a report identifying current users of MCCS. This report is sent to regional managers for review. We reviewed the report for the Ontario region and found that 14 of the 27 Ontario users had not logged onto MCCS since 2005.

In addition, no formal procedures were found for granting and approving privileges for the DBAs or for Super User Access to the operating system. DBA accounts are administered by the CIO, not BPMD, and are not subject to the same level of supervision as MCCS user accounts. The difference in the level of supervision is because the DBA requires direct access to the MCCS Oracle database whereas MCCS users do not have access to the MCCS Oracle database. The department is exposed to the risk that a member of the DBA team or a Super User may perform tasks that are not detected and are not within the expectations of the MCCS management team. There is also a risk of unauthorized access to the MCCS database.

Recommendation No. 3

It is recommended that the Director General of Business Planning and Management Directorate (BPMD), First Nations Inuit Health Branch (FNIHB):

a) request that the CIO implement and document standard DBA operating procedures for approving privileges for DBAs and Super User Access to the operating system; and

b) instruct all regions to carefully review the date of last access of users and deactivate user accounts for users not accessing MCCS over a predetermined number of months.

Management Response

a) Accept. The Director General, BPMD has consulted the CIO and they will take responsibility for implementing and documenting of standard operating procedures for approving privileges for DBAs and Super Users.

b) Accept. Regional account managers will continue to perform the six month review of all accounts in their region with emphasis on the date of last access.

Data Integrity Provisions

Procedures should exist to ensure that, where applicable, application programs contain provisions which routinely verify the tasks performed by the software to help ensure data integrity, and to provide the restoration of the integrity through rollback (a database management software feature that reverses the current transaction out of the database, returning the data to its former state). A rollback is performed when transaction processing fails at some point, and it is necessary to start over. Routine procedures that help to ensure data integrity should be documented.

Procedures for maintaining data integrity are not documented because the department has no policy enforcing the documentation of standard DBA operating procedures. There is a risk that if the DBA or their backup are not available, a replacement DBA may have to spend considerable time investigating which database maintenance procedures are required and how to perform the maintenance procedures. This may cause delays in database recovery.

Recommendation No. 4

It is recommended that the Director General of Business Planning and Management Directorate (BPMD), First Nations Inuit Health Branch (FNIHB), request that the CIO document all the procedures for ensuring data integrity and correcting database problems.

Management Response

Accept. The Director General, BPMD has consulted the CIO and they will prepare procedures for ensuring data integrity and correcting database problems.

Off-site Backup Storage

Off-site storage of critical backup media, documentation and other IT resources should be established to support recovery and business continuity plans.

Formalized standard operating procedures for off-site backup storage do not exist. We interviewed the Oracle DBA for MCCS and also interviewed staff in the Network Systems Services Centre (NSSC) server group. We learned that backup tapes are created and rotated daily, weekly, monthly and annually. The daily and weekly rotations are kept on site at the data centre. The monthly and annual tapes are kept off-site. NSSC tracks the tapes that were recalled or shipped between the data centre and the off-site storage location.

We found no evidence of reports or logs created to ensure that successful backups were actually performed. The lack of reports or logs is due to the lack of requirement to document backup procedures. There is a risk that specific data archives may not be at the off-site facility or available for restore purposes when needed.

Recommendation No. 5

It is recommended that the Director General of Business Planning and Management Directorate (BPMD), First Nations Inuit Health Branch (FNIHB) request that the CIO document backup and off-site storage procedures. These procedures should include at least:

- *instructions for performing the backups;*
- *instructions for verifying that the backup worked properly;*
- *instructions for verifying that the backup file device can be used to successfully restore the database(s);*
- *instructions for properly labeling the backup file device;*
- *instructions for shipping the backup file device for the off-site storage*
- *instructions for receiving the backup file device back from off-site storage;*
- *retention periods for the backup storage device; and*

- *instructions for monitoring the backup process and transmission of backup media between the data centre and the off-site storage facility.*

Management Response

Accept. The Director General, BPMD has consulted the CIO, and they will provide documentation for database backup and off-site storage procedures.

Systems Development Life Cycle Procedures

Health Canada's System Development Life Cycle (SDLC) methodology requires that:

- adequate mechanisms for defining and documenting the input requirements for any application or system development or modification project;
- all external and internal interfaces are properly specified, designed and documented; and
- adequate mechanisms exist for defining and documenting the output requirements for any application or system development or modification project.

There is no formal documented SDLC methodology. Mechanisms for defining and documenting input requirements or input changes are done via the MCCS tracking database. MCCS is a Commercial Off The Shelf (COTS) application originally customized to meet the needs of FNIHB. Any source code changes and table changes must be performed by the vendor. The MCCS support team can only make limited changes to the values of certain editable data fields. No input or output field level changes can be performed since SAP required input fields cannot be changed and MCCS output file formats are hard coded in MCCS and can only be changed by the vendor of MCCS.

Although the external interface formats to SAP have been predetermined and implemented, there are no general guidelines or methodology to specify how external and internal MCCS interfaces are to be specified, designed or documented in the future. Also, there are no mechanisms for defining and documenting the MCCS output requirements to SAP. Without a documented SDLC there is a risk that in a MCCS development or maintenance project business requirements and functionality for data interfaces may be missed or implemented incorrectly.

Recommendation No. 6

It is recommended that the Director General of Business Planning and Management Directorate (BPMD), First Nations Inuit Health Branch (FNIHB), use an SDLC methodology to document the MCCS-SAP interface.

Management Response

Accept. A document will be prepared to identify and describe the current MCCS-SAP interface process.