Health Canada Santé Canada

Final Audit Report

Audit of Data Integrity
Lotus Notes APICS and Acquisition Card Applications

June 2008

Table of Contents

Executive Summary

The Automated Procurement Initiation and Commitment Application (APICS) is a Lotus Notes application used by acquisition cardholders and their delegates to create commitments in the SAP system for purchases made using an Acquisition Card. The Lotus Notes Acquisition Card application is used to reconcile the monthly statement from the banks and provide the necessary coding for transactions to be sent to SAP, which is the Department's financial system. Information from APICS can be used in the reconciliation process to match transactions against previous commitments created in APICS.

Health Canada's Framework for Integrated Resource Management System (FIRMS) uses SAP for entering transactions, interfacing with various internal applications such as the Lotus Notes APICS and Acquisition Card applications. The data within SAP is used to generate financial and management reports that are then used to effectively manage the Department's resources and assets. APICS/Acquisition Card applications processed approximately $80 million in acquisition card transactions.

The two objectives of the audit were to:

a) determine the quality of the data, in terms of completeness and accuracy, of applications that interface with FIRMS/SAP; and

b) provide an overall assessment of the internal control environment around those applications.

The Audit and Accountability Bureau conducted the review in accordance with the Government of Canada's *Policy on Internal Audit*. These are two of several other feeder applications, which interface with SAP, that were included in the audit plan.

The information in APICS application/database is not complete because some commitments remain open and never get closed in APICS. The commitment data gets closed directly into SAP for those commitments left open in APICS. The Acquisition Card application/database, which updates acquisition card transaction data in SAP, is complete and accurate. The general controls environment is working well however, the Lotus Notes APICS and Acquisition Card applications procedures must be improved to address periodic review and confirmation of access rights (including super user) to these applications.

Introduction

Background

Automated Procurement Initiation and Commitment Application (APICS) is a Lotus Notes application used by acquisition cardholders and their delegates to create commitments in SAP for purchases made using an acquisition card. The Lotus Notes Acquisition Card application is used to reconcile the monthly statement from the banks and provide the necessary coding for transactions to be sent to SAP. Information from APICS can be used in the reconciliation process to match transactions against open commitments in APICS. The Lotus Notes Acquisition Card application is used to reconcile the monthly statement from the banks and provide the necessary coding for transactions to be sent to SAP. Information from APICS can be used in the reconciliation process to match transactions against previous commitments created in APICS.

Health Canada's Framework for Integrated Resource Management System (FIRMS) uses SAP for entering transactions and interfacing with various internal applications such as the Lotus Notes APICS and Acquisition Card applications. The data within SAP is used to generate financial and management reports that are then used to effectively manage the Department's resources and assets.

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

Objectives

The focus of the audit was to review the Lotus Notes APICS and Acquisition Card applications interface with FIRMS/SAP. The two objectives of this audit are 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 those systems.

The lines of enquiry for the audit include:

- **Completeness and Accuracy of Data**
  - Input/Processing/Output Controls;
  - controls to ensure that all data was successfully interfaced;
  - error processing; and,
  - segregation of responsibilities.

- **General Controls Environment**
  - problem Management;
  - access controls; and
  - off-site backup and Restoration / IT integrity provisions in application program software.

Scope and Approach

The scope of this audit covers the APICS and Acquisition Card Lotus Notes applications that interface with FIRMS/SAP. The audit was conducted in the National Capital Region. The period assessed was from January 1, 2006 to December 31, 2006.

The audit was conducted in accordance with:

- ISACA's COBIT (Control Objectives for Information and Related Technology) which is an IT governance model; and

- Treasury Board's Internal Audit Policy.

The audit consisted mainly of interviews with functional experts within Health Canada, an examination of relevant documentation and tests of the general computer and application controls for the APICS and Acquisition Card applications and their interface with SAP.

The audit included examination and validation of data inputs, logical access controls and authorization and exception handling and logging. Documentation reviewed included user manuals, training manuals and technical manuals related to interfaces. Evidence gathered and analyzed consisted of data transferred from the APICS and Acquisition Card applications to SAP during the calendar year 2006. Fifty four (54) commitments from the 2006 APICS transactions were extracted. We verified this information and found that it was consistent across the APICS, the Acquisition Card and SAP application databases. Specific tests were conducted to verify the information contained in the various databases to the actual input information.

Findings, Recommendations and Management Responses

Completeness and Accuracy of Data

Input/Processing/Output Controls

Procedures must be in place to ensure that source documents expected are received, all required data received are processed and all output required is prepared and delivered.

The APICS application is used to commit funds that will be spent using the acquisition cards. The reinforcement of the requirement to use APICS to commit funds to be spent using the acquisition card is not strong. Users can enter information by hand in the Acquisition Card Database and do not have to match the transactions to a commitment in APICS when doing the reconciliation, which lessens the impact of not using APICS. Also, there is no control over the reconciliation of the commitment information. Some information is entered in APICS and doesn't get cancelled when not used or the commitments get closed directly in SAP, which causes the APICS entry to be left open. Commitments can be closed and modified directly through SAP, so information in APICS is not the most current information or system of record.

Not all commitment data is input into the APICS database and therefore does not provide a complete source of information. At the time of fieldwork, the current Acquisition Card Policy had not adequately addressed procedures for processing acquisition card data, specifically balancing of acquisition card commitment data and acquisition card statement reconciliation. The New Acquisition Card Policy (September 7, 2007), has introduced more complete procedures to address the reconciliation of commitment data in APICS.

Error processing

Procedures must exist for the correction and resubmission of erroneous data. Also, procedures must exist for reviewing the accuracy of output reports. Procedures must be in place for the identification and handling of errors contained in the output.

Input errors are recorded in each transaction document. There is no control to ensure that APICS commitments are followed up. This is left up to the discretion of the authors responsible for the commitment. There is a risk that rejected commitments registered in APICS may never be addressed. As stated above, the APICS database is not a reliable and complete source of information.

In the Acquisition Card application, input errors are also recorded in each transaction document. Out of the 21 errors present at time of testing, we examined 12. Nine of the 12 errors were corrected in a timely manner. Two of the 3 have since been addressed, as

they were Payment at Year End (PAYE). As for the 3rd one, the credit card has since been cancelled and the error was left unaddressed.

Based on test results indicated above, complimented with the availability of an APICS help function, training material and a FIRMS training quick reference guide, we believe that there is adequate documentation for acquisition card holders to manage and process error related transactions.

Segregation of responsibilities

Procedures must exist to ensure that separation of duties is maintained and work performed is routinely verified with the person's role. The segregation of duties in place must also address the preparation and approval of source documents by only authorized personnel.

The current Acquisition Card policy and procedures in place at the time of the fieldwork did not clearly address how "separation of duties" is to be maintained. Out of a sample of 31 approved (Sect 34) reconciliation coding sheets, 3 of the sample had Section 34 approval being done by the cardholder not the cardholder manager (CCM).

There was a problem in the definition of the segregation of duties with the individuals. Roles needed to be clearly defined. Some cardholders have a delegation of section 34, but should not approve their own statements. On April 11, 2007, an HC Broadcast news stated that "Effective immediately, all acquisition card statement reconciliation must be approved under Section 34 by the Cost Centre Manager (CCM), or, if the CCM is a cardholder, by the CCM's supervisor". CFOB has informed AAB that this issue will be reinforced to all existing and new acquisition cardholders in future training. Our sample was taken previous to that broadcast. Revamped procedural changes within the New Acquisition Card Policy should clarify roles of the acquisition card holder and their supervisor.

General Controls Environment

Problem Management

Management has implemented a problem management system to ensure that all operational events that are not part of the standard operation (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner. Emergency program change procedures are promptly tested, documented, approved and reported.

The current Magic System is used to track calls made to the Help Desk. Once the Help Desk has analyzed the problem and determined that it is an application problem, the call is assigned to the FIRMS business unit. At this stage, the call is closed.

FIRMS is supported by an issues database and a Development Requests (DR) database. The DR database system is self-documenting and contains all the necessary steps to ensure that the work is properly tracked and follows a standard SDLC methodology. There are adequate controls to ensure that the problem is adequately addressed.

Identity Management and Management Review of User Accounts

All users and their activity on the APICS and Acquisition Card applications are uniquely identifiable. User access rights are requested by user management, approved by application owner and implemented by the security-responsible person.

Access to the APICS/Acquisition card application is tied to the signature card database. Granting and denial of these accesses are well documented in the Acquisition Card Policy However, the Acquisition Card Policy does not address procedures for periodic review and confirmation of access rights by regular and super users to the APICS/ Acquisition Card applications and databases. This would be accomplished by verifying the acquisition card and the signature card databases.

There is a risk of unauthorized access to APICS /Acquisition Card data from an application administration perspective since no formal procedures for administering super user access to databases are available. There is also a risk that users who no longer need access or whose job responsibilities have changed may still have access to the APICS and Acquisition Card applications.

Recommendation No. 1

It is recommended that the Chief Financial Officer as the Business Owner, in conjunction with the Chief Information Officer, Information Management Services Directorate, ensure that APICS and Acquisition card policies and procedures address procedures for periodic review and confirmation of access rights to the APICS/ Acquisition Card databases. This also includes super user access and review.

Management Response

The Chief Financial Officer accepts the recommendation of the audit. As a result of the audit, the Framework for Integrated Resource Management Systems (FIRMS) has instituted a procedure, whereby the Access Control Lists for both the APICS and Acquisition Card databases are to be reviewed as part of the Year-End procedures. The review will involve looking at the members of any group who has rights beyond those of a normal user (i.e. manager's rights, administrative rights), and requesting verification of names from the business contacts. This review will be over and above the ad-hoc reviews that occur whenever FIRMS are specifically asked to add or remove a user from the Access Control Lists.

Appendix A: APICS and Acquisition Card Applications