Health Canada Santé Canada

Final Audit Report

Audit of Data Integrity
Lotus Notes Grants & Contributions System

April 2008

Table of Contents

Executive Summary

The Lotus Notes Grants & Contribution (G&C) System was developed by the previous Health Promotion and Programs Branch (HPPB), now part of Public Health Agency Canada (PHAC), to manage and monitor all grants and contributions (G&C) activities. The system is used on a daily basis as a project management tracking tool by Health Canada front-line staff (all Branches except FNIHB) and to generate G&C projects reports of a statistical, financial and narrative nature. The System contains information on projects funded through G&C as well as financial data on commitments and payments that interface with the Departmental Financial System (SAP).

Health Canada's Framework for Integrated Resource Management System (FIRMS) uses SAP for entering transactions, interfacing with various internal systems such as the Lotus Notes Grants and Contribution system. The data within SAP is used to generate financial and management reports which are then used to effectively manage the Department's resources and assets. The total value of all 2005-06 commitments processed in the Lotus Notes G&C System is approximately $502 million.

The two objectives of the audit were to:

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

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

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

In conclusion, no major data integrity issues were identified during the course of this audit. However, the Lotus Notes G&C system does not generate control totals to compare input and outputs with SAP. This is a necessary control required to balance the data that is being interfaced from Lotus Notes G&C with SAP. There is risk of not knowing if all of the data has been interfaced with SAP. Overall the controls environment is operating satisfactorily; however, improvements to the documentation regarding operating procedures are needed to ensure consistency of the data.

Introduction

Background

The Lotus Notes Grants & Contribution (G&C) System was developed by the previous Health Promotion and Programs Branch (HPPB), now part of Public Health Agency Canada (PHAC), to manage and monitor all grants and contributions (G&C) activities. The system is used on a daily basis as a project management tracking tool by Health Canada front-line staff (all Branches except FNIHB) and to generate G&C projects reports of a statistical, financial and narrative nature.

The System contains information on projects funded through (G&C) as well as financial data on commitments and payments that interface with the Departmental Financial System (SAP). The total value of all 2005-06 commitments processed in the Lotus Notes G&C System is approximately $502 million.

Health Canada's Framework for Integrated Resource Management System (FIRMS) uses SAP for entering transactions, interfacing with various internal systems such as the Lotus Notes Grants and Contribution system. The data within SAP is used to generate financial and management reports which is then used to effectively manage the Department's resources and assets.

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.*

Objectives

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 the Data**
  - automated field edits in the Lotus Notes G&C system;
  - controls to ensure that all data was successfully interfaced;
  - transaction controls;
  - error processing;
  - segregation of responsibilities;

- **General Controls Environment**
  - access controls;
  - change Management;
  - backup and restore;
  - problem reporting and resolution;
  - internal monitoring; and
  - configuration Management

Scope and Approach

The scope of this audit covers the Grants and Contributions system that interfaces with FIRMS/SAP.

The audit for the Lotus Notes G&C System interface was conducted in the National Capital Region. The period assessed was from January 1, 2006 to December 31, 2006. The period assessed for the audit was the calendar year 2006 due to fact that the system processes multi-year contribution agreements which are based on calendar year rather than the government's fiscal year.

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 concerned with the Lotus Notes G&C system interface with SAP. There has been no testing of the Contribution Agreement Program.

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 Lotus Notes G&C system to SAP during the calendar year 2006. Specific tests were conducted to verify information contained in the files to the actual Program/Finance files.

A sample of 24 projects that interfaced between the Lotus Notes G&C system and SAP were tested. These files were selected from the calendar year 2006. Testing at the detail data field level could not be done as LN G&C interface program was not setup to retain this type of information after data that interfaced with SAP was completed. The G&C Centre of Excellence indicated that the processing required to retain all the detail data field information would degrade the performance of the Lotus Notes G&C system.

Findings, Recommendations and Management Response

Completeness and Accuracy of Data

Accuracy, Completeness and Authorization Checks

Input data should be subject to a variety of controls to check for accuracy, completeness and validity and edited as close to the point of origination as possible. Input data is subjected to minimal built in application controls for completeness, validity and accuracy.

Validity checks are done by visual inspection of the data entered and are subject to human error. Projects can be entered with incorrect funding and coding information and therefore have to be corrected after initial data entry. We also identified projects with funding that exceeded budgets.

Data entered in Lotus Notes G&C system is dependant on SAP for validity and error checking. When an error occurs, the error codes are sent back to the source of the data entry for rectification and the Logics Help Desk is informed that corrections are needed.

There is a continued risk that if stronger controls for entering amounts and financial coding are not introduced, then a percentage of projects will always have to have financial information re-entered. This may result in delays to processing of payments and incomplete and/or inaccurate data.

Recommendation No. 1

The Director General, Financial Operations Directorate, Chief Financial Officer Branch should ensure that the Lotus Notes G&C system is updated to include more automated edits.

Management Response

Accept with conditions. Updating the LN G&C system to include more automated edits would require a significant effort in redesigning the interface with SAP. However, a study is currently underway to identify a recommended automated G&C system for the entire department. The increased automated edits will be incorporated into the implementation of the departmental solution. In the interim, the existing controls within the G&C Centre of Expertise (CoE) will continue to function. These include the automated identification of failed interface transactions and the manual rectification of problems by either the CoE or the transaction originator. Furthermore, since these transactions are tracked daily, the risks to delaying the processing of payments are minimal.

Data Error Handling

Procedures should exist and are followed for the correction and resubmission of erroneous data.

Formal procedures do not exist for the correction and resubmission of data input errors. However erroneous data input may be found through a compensating control when SAP attempts to validate a Lotus Notes G&C transaction. When errors are identified, SAP passes the error message back to the Batch Notes Interface to SAP (BNITS) program, which logs the error and then passes it back to the originating Lotus Notes G&C project document.

The Lotus Notes G&C Help Desk checks for errors on an ad hoc basis and if problems are found the Help Desk will either rectify the problem (if they have the authority) or pass it along to the user who originated the problem. Errors that are not found expose the department to the risk of inaccurate and/or incomplete data.

Error handling procedures should also exist during data origination to reasonably ensure that errors and irregularities are detected, reported and corrected. Formal procedures to review for errors during data origination do not exist.

There is a risk that delays may be experienced in processing related SAP commitments due to Lotus Notes G&C source document errors not being addressed in a timely manner. By not addressing LNG&C source document errors in a timely manner the department is at risk of having inaccurate and/or incomplete data. The Lotus Notes G&C Help Desk is planning to initiate daily error reporting where the Help Desk will either rectify the problem (if they have the authority) or pass it along to the user who the problem originated with for resolution.

Recommendation No. 2

The Director General, Financial Operations Directorate, Chief Financial Officer Branch should document input error handling procedures. At a minimum these procedures should include:

- *detecting errors;*
- *resolving errors;*
- *escalating errors; and*
- *controlling errors to ensure they are accurately re-input back into the system.*

Management Response

Agreed. As indicated in the response to Recommendation No. 1, the Lotus Notes G&C Help Desk has already initiated daily error reporting. The plan is that the formal documentation of the procedures will be completed by March 31, 2008.

Data Processing Integrity

Procedures should exist to ensure that separation of duties is maintained and work performed is routinely verified with the roles of individuals.

Formal documented procedures do not exist to ensure that separation of duties and work is maintained, performed, and routinely verified with an individual's role. Financial officers have the ability, through editor access, to update financial data through amendments to G&C related projects. The department is therefore at risk of people performing conflicting roles. This can result in inaccurate data in the Lotus Notes G&C data if one person enters payment information and is then able to change the information without appropriate authorization.

Recommendation No. 3

The Director General, Financial Operations Directorate, Chief Financial Officer Branch should ensure that adequate separation of duties is maintained. The procedures should include a definition of roles performed by each type of user and roles that should not be performed by each type of user.

Management Response

Agreed, however, explaining user roles and responsibilities has always been a component of the LN G&C System Training; which is offered on numerous occasions throughout the year. Included in the training documentation is the requirement for a proper separation of duties as well as the definitions of roles that should and should not be performed by each type of user.

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.

Without control totals, management is at risk of not knowing whether all the information from Lotus Notes G&C was actually interfaced with 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.

Payment transactions are reconciled every month at the beginning of each period. If errors are found a standard email is sent to the Financial Editor(s) of each specific project to request that corrections be made to the project. Common errors are documented to ensure that proper steps are taken to avoid recurrence and included as part of the Lotus Notes G&C database training curriculum.

There is insufficient follow up on error corrections which could potentially cause data to be inaccurate or incomplete.

Recommendation No. 4

The Director General, Financial Operations Directorate, Chief Financial Officer Branch should incorporate control totals into the Lotus Notes G&C reconciliation process and implement procedures and document the procedures to ensure that errors are corrected and resubmitted on a timely basis.

Management Response

Agreed. Monthly reconciliations are now being done.

General Controls Environment

Change Management (Input, Interface and Output Requirements Definition and Documentation)

The organization'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.

The details of the SDLC methodology in respect to documentation requirements and expectations for input/output and interfaces are not specified. The details of the testing that have been performed (such as integration and user acceptance environments) prior to being put into production (e.g. Development, and Quality Assurance) are not documented.

The current Lotus Notes G&C SDLC methodology includes the following steps:

- step 1: Investigation of the Request, Gather Business Requirements;
- step 2: Development & Testing;
- step 3: Promotion from development to Quality Assurance (QA);
- step 4: Client Acceptance Testing; and
- step 5: Development.

A sample of seven development requests was examined. From this sample, three out of seven had vague or non existent requirements.

The department is at risk of excessive downtime caused by the development team's efforts required to specifically define requirements by management. There is also a risk that functions may be developed without management approval and that development projects undertaken may

not yield the functional and quality expectations of the client. The excessive downtime and the possible implementation of unauthorized changes can result in inaccurate, incomplete data.

Recommendation No. 5

The Director General, Financial Operations Directorate, Chief Financial Officer Branch should:

a) implement procedures to ensure input/output and interface specifications are documented and that there is approval at the appropriate level; and
b) document detail requirements for testing.

Management Response

Agreed. Significant improvements have already been implemented to address system changes/enhancements. The CoE has implemented a formal "Systems Development Request Process"; which includes the requirement that all requests be approved by the Team Lead, Business and Systems, prior to being submitted to the Systems Development Team.

At the time of the audit, all systems development requests were being (and continue to be) initiated through the "Corporate Services Branch (CSB) Request" database, which is used to record, track, estimate and test all development requirements.

Furthermore, the "CSB Request" database also allows for the prioritization of development requests by degree of urgency. Emergency fixes are identified as the first order of priority.

Proper utilization of the aforementioned database should mitigate the risks identified by this audit observation.

User Access Rights

User access rights to systems is 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 the security-responsible person. Procedures should exist to also periodically review and confirm access rights.

User access rights to the Lotus Notes G&C system are not formally requested or formally approved. It was observed that the management of user accounts for the Lotus Notes G&C system was problematic the way it was designed. A request to create a new user account or to change an existing user account can be made either verbally or sent via e-mail and can be made by the actual user requiring access. Also, there is no periodic review of user access rights and no procedure exists to periodically review or confirm access rights.

Access to the Lotus Notes G&C system is not based on defined documented business needs and job requirements. There are no formal procedures to ensure that user access rights are requested, approved and granted based on documented and defined job responsibility.

There is a risk to the department that users with inappropriate access rights may gain access to the LNGs&Cs application which can result in unauthorized input or changes to data causing the data to be inaccurate and/or incomplete.

Recommendation No. 6

The Director General Financial Operations Directorate of Chief Financial Officer Branch should implement and document formal procedures for:

a) requesting that new user account and changing/deleting user accounts be based on job responsibility; and
b) regularly reviewing user access to the Lotus Notes G&C System be based on job responsibility.

Management Response

Agreed. The CoE is planning to implement a formal user account request/change process within the next 6 months. This process will be based upon job responsibility.

The CoE has implemented a "User Activity Report Process" whereby user activity/non-activity is be monitored on a monthly basis. Accounts no longer required are deactivated.

Problem Reporting and Resolution

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

Formal documented procedures for managing problems and implementing emergency changes do not exist. There are no documented procedures requiring business approval for correcting some types of system problems encountered during production.

This exposes the department to the risk that emergency changes may not always get processed in an appropriate and consistent manner which may lead to inaccurate and incomplete data.

Recommendation No. 7

The Director General Financial Operations Directorate of Chief Financial Operations Branch should implement and document procedures for managing problems, monitoring changes and implementing emergency changes. These procedures should include but not be limited to:

- *identifying changes;*
- *approving changes;*
- *implementing emergency fixes; and*
- *estimating changes.*

Management Response

Agreed. Please refer to the Management response to Recommendation No. 5.

Internal Control Monitoring

Management should monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, reconciliations and other routine actions. Internal controls should operate promptly to highlight errors and inconsistencies, and to ensure that these are corrected before they impact production and delivery.

Internal controls are not preventive and don't operate at a pace that promptly highlights errors and inconsistencies. Therefore there are no guarantees that processing will not be impacted due to errors and inconsistencies.

We observed that the only internal control monitoring done is through the monthly SAP-Lotus Notes G&C reconciliation process. Apart from this activity, there is no monitoring of the effectiveness of internal controls. There is a risk that internal controls are not generally operating as effectively as they appear and that inconsistencies may not be identified until the end of the month during the monthly reconciliation process. This can result in inaccurate and/or incomplete data residing on the LNG&C database.

Recommendation No. 8

The Director General Financial Operations Directorate of Chief Financial Officer Branch should document and implement more frequent, regular monitoring procedures.

Management Response

Agreed. As per the Management response to Recommendation No. 4, the monthly reconciliation process should be sufficient to properly mitigate internal control risks.