OFFICE OF THE
Auditor General
of British Columbia

BACKGROUNDER

December 12, 2006

Audit of Government's Corporate Accounting System: Part 2

Second report on the assessment of controls of the Corporate Accounting System

What is the corporate accounting system?

All government ministries and numerous agencies enter their financial information into one central accounting and financial reporting system, the Corporate Accounting System (CAS). By connecting to the shared government network, staff in offices throughout the province can access CAS and enter transactions. All government expenses and revenue – about $27 billion and $29 billion, respectively, in 2005/2006 - are processed through this system. This represents more than 4 million expenditure transactions, more than 2 million balance sheet transactions, and about 620,000 revenue transactions. As well, more than 275,000 individuals and businesses are listed in the system, as suppliers that could receive payments from government for goods or services.

Why is control of CAS critical?

Transactions, initiated from locations across the province, are used to pay suppliers, record revenue collections, and generate reports that help management monitor spending levels and make business decisions. And, once summarized, these transactions are used to produce government's financial statements.

The sound operation of many of government's key business functions therefore depends on:

- every transaction entered and processed in CAS being authorized (valid), accurate and complete; and
- the information generated by the system being accurate, complete, timely and continuously available.

Incorrect entries, as a result of human error or unauthorized access to the system, could potentially result in incorrect payments, as well as critical business functions (such as financial reporting) being compromised. The potential for these problems is not unique to CAS. Every computing system faces

similar risks. The only way to minimize these risks (and to maximize the likelihood of detecting problems if they do occur) is through a strong control environment.

. . . 2

CAS is highly dependent on four basic types of controls:

1. manual controls – management controls such as report monitoring and manual reconciliations and approvals,
2. inherent controls – controls built into the operation of the system, such as edit and validation routines,
3. configuration settings – customized options to control and direct processing operations, and
4. logical access security – restrictions on access to system functions.

There are some built-in, automated features to ensure data entered meets predefined criteria. One example is the use of edit routines, such as matching the purchase order totals to invoice totals to validate invoices for payment. Nevertheless, because many of these features can be pre-configured in Oracle Financials – meaning that previously set parameters can be reset – it is critical that proper manual controls, such as change management and security policies and procedures, also be in place.

All systems of internal control involve accepting some level of risk. It is management's role to assess the increased risks associated with control weaknesses identified during the audit and either implement procedures to minimize those risks or develop plans to manage them.

What we looked at

In our 2005 report *Audit of the Government's Corporate Accounting System: Part 1*, we presented our findings on controls over the governance of CAS and the CAS operating system and central database.

In the report on Part 2 of our audit of the CAS application (issued today), we focused on the following areas – the administration of security over access to the accounting software, and certain controls over two significant components of the accounting software: the general ledger module and the purchasing/accounts payable modules.

We examined the controls in place designed to ensure: (1) access to the system and to specific activities was appropriately restricted; (2) transaction processing in the general ledger module was complete, accurate, and timely; and (3) transactions in the purchasing/accounts payable modules were valid. A lack of proper controls in these areas could significantly affect the reliability of government's financial information.

This report was issued on behalf of the Office by the Deputy Auditor General, Errol Price. The Acting Auditor General, Mr Arn van Iersel, in his previous capacity as Comptroller General for British Columbia, had significant influence on the Corporate Accounting System, which was the subject of this audit. The Acting Auditor General was not therefore involved in the audit or the preparation of the report.

. . . 3

Key findings and recommendations

We concluded that, with some exceptions, proper control procedures were in place and being followed to ensure that financial information is processed completely, accurately and on a timely basis. However, we identified several key areas where we felt that controls were not adequate to address the following risks.

- The risk that incorrect access to the accounting system could jeopardize its integrity

  - *Corporate Accounting Services should take a more proactive role in ensuring all access is appropriate by alerting ministries of possible problems with user access; and*
  - *procedures should be established to communicate staff changes to security administrators in a timely manner to ensure effective user access change management, and to periodically review user access levels to ensure access granted remains appropriate based on users' positions.*

- The risk that the chart of accounts could be inaccurately coded resulting in inaccurate financial reporting

  - *Monitoring activities should be formalized and carried out by the Office of the Comptroller General (OCG) to ensure the chart data remains current and relevant.*

- The risk that payments could be directed to incorrect suppliers

  - *Corporate Accounting Services should establish formal policies restricting further set-up of generic suppliers and formalize a plan to establish a well-defined approach for using, managing and updating existing generic supplier records.*

- The risk that details of payments to some suppliers are not fully reported in the schedule of supplier payments published with government's annual financial statements

  - *OCG should establish clear criteria for monitoring and compliance activities to ensure that the block supplier data remains current and relevant.*

. . . 4

- The risk that electronic payments could be directed to fraudulent suppliers

  - *policies and procedures should be established to define clearly a ministry's role and responsibilities in the bank account maintenance process, and to govern the extent of ministry review required for ensuring the completeness and accuracy of banking information obtained;*
  - *OCG should communicate effectively to ministries the risks associated with banking activities and advise them how to detect the potential threats and to ensure that controls are functioning properly to address them; and*
  - *management at Corporate Accounting Services should formalize procedures to monitor all supplier linkages to bank accounts and compare the details of the reported activities to source documents to ensure there are no unauthorized or inappropriate bank account linkages*.

- The risk that there is opportunity for unauthorized transactions

  · *Corporate Accounting Services should explore the feasibility of requiring approval from expense authorities when manual changes are made to suppliers' cheque mailing addresses to prevent unauthorized changes. Guidance should also be established to ensure proper validation procedures are carried out when approving these changes; and*

  · *management should require expense authorities to review procurement transactions when supplier information is subsequently added to purchase orders or changed, to ensure the appropriateness of the suppliers used for procuring the goods and services.*

- The risk that monitoring procedures are not sufficient to detect errors or fraud in ministry expenses

  - *OCG should take on the initial responsibility of effectively communicating with ministries the risks of potential fraud in purchase and accounts payable transactions and advising them on how to detect potential threats resulting from these risks*.