News Release

Report

Audit of the Government's Corporate Accounting System: Part 1

Backgrounder
June 28, 2005

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 payments and revenue – about $25 billion and $23 billion, respectively, in 2003/2004 - are processed through CAS. These amounts are the sum of the large number of transactions that are recorded and processed in the system: over 4 million expenditure transactions, over 2 million asset and liability transactions, and about 700,000 revenue transactions.

As shown in the following diagram, the main components of CAS are the UNIX operating system, the Oracle database and the Oracle Financials accounting software.

Why is control of CAS critical?
The business functions of government, such as payments to suppliers, rely on the accuracy, completeness and validity of the transactions entered and processed in CAS and on the continuous availability of the information generated.

Incorrect data in CAS, as a result of human error or unauthorized access to the system, could potentially result in incorrect payments being made. And system maintenance problems or a lack of processing capacity could result in government staff being unable to access CAS and in disruptions to payments to government suppliers and employees.

These problems are not unique to CAS; every computing system faces similar risks. Any operating system could fail to meet current requirements or keep up with future business requirements, causing performance or availability problems. Unauthorized changes could be made to an operating system, affecting security, availability or performance. Someone could gain unauthorized access and view or change the information on the system. Or the building housing the system could be compromised by unauthorized access or a disaster, leading to system unavailability or the loss of information.

A strong control environment can lessen these risks. Through a combination of *governance* controls and system

controls, these risks can be prevented from occurring, or be detected if they do.

Governance controls are organizational requirements implemented by management, such as the development of policies, procedures and standards, followed by monitoring for compliance. These controls direct responsibilities for IT planning, risk management and control, business continuation planning, and other responsibilities that require a centralized direction.

System controls are controls over the operating system, the central database and the accounting software that help to ensure continuous service, accurate and complete processing, and only authorized access to the system and government information.

Both types of controls must be assessed, since the effectiveness of one type of control can enhance or reduce the effectiveness of the other. For example, management can reduce the impact of a deficiency in a system control by using governance controls to monitor events and analyze outcomes, following-up to ascertain the reason. On the other hand, strong system controls over access can be compromised if management does not develop and enforce policies, such as those for issuing access to new users.

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

Top of Page