2005/2006 : Report 3

OFFICE OF THE

Auditor General of British Columbia

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

June 2005

Canadian Cataloguing in Publication Data

British Columbia. Office of the Auditor General.

Audit of the government's Corporate Accounting System: part 1

(Report ; 2005/2006: 3)

Running title: CAS review report 1.

ISBN 0–7726–5376–3

1. Corporate Accounting System (Computer system). 2. Finance, Public – British Columbia – Data processing – Evaluation. 3. Administrative agencies - British Columbia – Accounting – Data processing – Evaluation. I . Title. II. Title: Audit of the government's Corporate Accounting System. III. Title: CAS review report 1. IV. Series: British Columbia. Office of the Auditor General. Report ; 2005/2006: 3.

HJ9921.Z9B74 2005 352.4'3'09711 C2005–960128–0

LOCATION:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

OFFICE HOURS:
Monday to Friday
8:30 a.m. – 4:30 p.m.

TELEPHONE:
250 387–6803
Toll free through Enquiry BC at: 1 800 663–7867
In Vancouver dial 660–2421

FAX: 250 387–1230

E–MAIL: bcauditor@bcauditor.com

WEBSITE:
This report and others are available at our Website, which also contains further information about the Office: http://bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my 2005/2006 Report 3: Audit of the Government's Corporate Accounting System: Part 1.

Wayne Strelioff, FCA
Auditor General

Victoria, British Columbia
June 2005

copy: Mr. E. George MacMinn, Q.C.
Clerk of the Legislative Assembly

Table of Contents

Acknowledgements

Audit Team

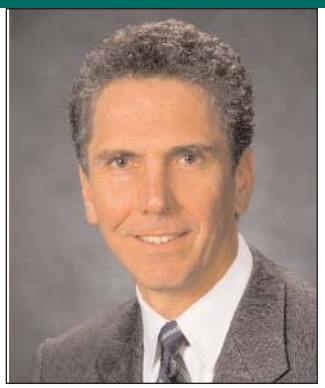
Bill Gilhooly

Faye Fletcher

Pam Hamilton

Joji Fortin

Auditor General's Comments



Wayne Strelioff, FCA
Auditor General

All government ministries and many agencies enter their financial information into one central accounting and financial reporting system, the Corporate Accounting System (CAS). Implemented on April 1, 2001, CAS gives the government the ability to perform on-line, real-time processing.

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 recorded through CAS. These amounts are the sum of the large number of transactions that are recorded in the system: over 4 million expenditure transactions, over 2 million balance sheet transactions and about 700,000 revenue transactions.

The central accounting system for all of government, CAS is a very large and complex system. Over 260,000 suppliers are listed in the database—individuals or businesses that could receive payments from the government for supplying goods or services. About 24,000 users, mainly government employees, have been granted access to CAS.

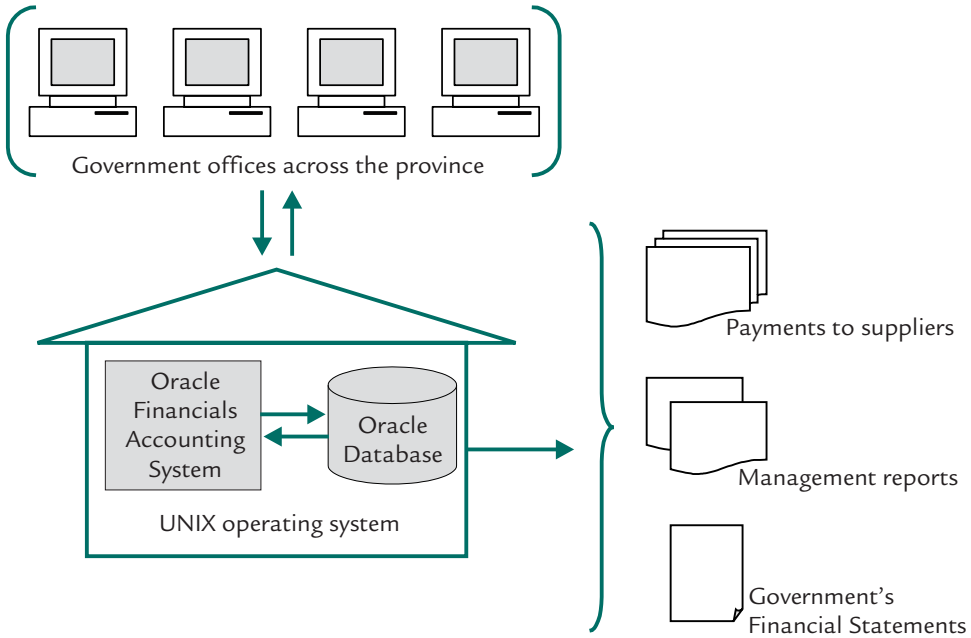
The main component of CAS is the Oracle Financials Accounting System. It runs on a UNIX operating system, using an Oracle database. This computing environment is shown in Exhibit 1.

Our audit is a multiyear project

The implementation and enhancement of CAS has been a multiyear project, carried out by the government in incremental steps. The CAS environment has been constantly changing, with new functions and hardware being added and existing hardware and software being upgraded. My approach has therefore been to conduct audits that span several years since CAS's initiation in 2001.

Exhibit 1

An overview of the CAS computing environment



We have audited the UNIX operating system and the Oracle database and we have reviewed CAS's governance framework. Currently, we are auditing the controls directly related to purchase, accounts payable and general ledger transactions.

This is our first report and includes the work done on UNIX, the database and governance controls. A second report, to be issued this fall, will include any follow-up work required as a result of this report, as well as our assessments of purchase, accounts payable and general ledger controls.

Control of CAS is 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 entries into CAS, as a result of human error or unauthorized access to the system, could impact several business functions and potentially result in incorrect payments. And system maintenance issues or insufficient processing capacity could result in government staff being unable to access CAS and in disruptions to payments to government suppliers and employees.

These potential 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, security and processing problems can be prevented, or be detected if they do occur.

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 information technology 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.

Our assessment of CAS covers both types of controls, 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 allowing 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.

Conclusion

Overall, I found the control environment we examined to be well managed.

We examined three main questions:

1. *Does senior management have a process in place to ensure that the information technology (IT) strategy for CAS is aligned with the government's business strategies and the CAS IT environment is managed in a way to ensure the continuous and effective delivery of service?*

   Senior management is responsible for maintaining adequate control and at the same time efficiently managing available resources to ensure that government can operate a central accounting service in a way that provides good value and an acceptable level of risk. Because CAS is a complex environment that provides services across government, governance involves communication with, and direction from, many interested parties. This has resulted in the interaction of numerous committees, made up of representatives from various levels of management within government.

   We found that management has appropriately set the objectives, established the policies and made the decisions needed to direct the planning and the organization of the CAS IT environment, the delivery and support of IT, and the monitoring and the evaluation of IT.

We are satisfied that, overall, senior management has a process in place to align the IT strategy for CAS with the government's business strategies and to manage the CAS IT environment in a way to ensure the continuous and effective delivery of service. In conducting our audit, we did note several less significant deficiencies in the control environment and make recommendations for improvements.

2. *Does the UNIX operating environment that CAS runs in, have adequate controls in place to ensure it is secure and will meet current and future business requirements?*

At the time of our initial high level assessment of the UNIX operating environment in the spring of 2002, there were adequate controls in place. However, during our audit of the Oracle database in the fall of 2003, we re-examined certain areas of the UNIX operating system and identified control weaknesses that could result in unauthorized access to the system or to government data.

We have not yet followed up on these issues because, between September 2004 and January 2005, CAS processing hardware (often referred to as servers) was being replaced or upgraded and the UNIX operating system was being upgraded. Data storage capacity was also being increased, as storage requirements have grown significantly with the retention of historical and other data. These are significant changes and will require a new follow-up assessment of the operating environment, which we will report on later this year.

3. *Is the Oracle database used by CAS adequately controlled to ensure that the information stored in it is secure and can be relied on?*

Management at Corporate Accounting Services has created a culture that is conducive to teamwork and to retaining dedicated, knowledgeable staff. My staff also noticed an increased awareness for security, with the organization having created a position for a dedicated Enterprise Security Officer.

We found that many needed controls over the Oracle database were in place. However, we did identify some control deficiencies that could jeopardize the integrity and reliability of the information stored in the database.

We were concerned that there was no record of the activity of the database administrators and specialized support staff, who can access all data. It is not possible to limit the access granted to these staff, as they need it in order to manage the operating system and database. (This is the same access that support staff in other businesses running the same type of system would have.) However, unlimited access increases the risk that fraudulent activity could occur and be undetected. Since this access cannot be limited, an audit log would serve to document staff activities, and allow monitoring of unusual activities.

We also found insufficient controls in place to appropriately restrict entry to CAS through the government network. Such restriction is usually achieved through specialized software and hardware (often called a firewall) that is set up to only allow authorized users into the system, and filters out data and messages according to specified security criteria or "firewall rules." We found inadequate controls over CAS's firewall rules and lack of a process that should ensure its operating continuously. Since our audit, management at Corporate Accounting Services has been actively improving the firewall security. Once the new firewall controls are in place, access to the CAS computing environment will be appropriately controlled from unauthorized access or malicious activities.

I wish to thank everyone for the cooperation my Office received in gathering the information for the audit. As well, I would like to acknowledge the hard work, professionalism and dedication of my staff in the production of this report.

Wayne Strelioff, FCA
Auditor General

Victoria, British Columbia
June 2005

Detailed Report

Background

All government ministries and many agencies enter their financial information into one central accounting and financial reporting system, the Corporate Accounting System (CAS). Implemented on April 1, 2001, CAS gives the government the ability to perform on-line, real-time processing. Transactions are initiated from various locations across the province and result in system-generated accounting entries. Management also obtains reports, based on these transactions, and uses them to monitor spending levels compared to budgets and make business decisions. As well, transactions are summarized to produce the government's financial statements.

The CAS IT environment

The main component of CAS is the Oracle Financials Accounting System (Oracle Financials). It operates within a UNIX operating system, using an Oracle database.

Oracle Financials is an enterprise resource planning (ERP) software application. An ERP application integrates departments and functions across an organization by taking common financial processes, such as purchasing, receiving, accounts payable, and payments, and processes all related transactions on a single computer system. In the past, organizations typically had three separate systems—one to handle purchasing, one to record accounts payable and one to record payments. The government, prior to CAS, also used a variety of computer systems for financial management, with some ministries having on-line access to enter transactions and others having to process transactions through a central batching system.

All transactions entered by ministries into Oracle Financials are recorded in the Oracle database, in thousands of data tables. In most cases, this database is updated simultaneously with each transaction entered on-line, using real-time processing. An entry to purchase goods, for example, can automatically create entries in accounts payable and the general ledger. If the initial entry is invalid, inaccurate or incomplete, several business functions can be significantly affected, including payments made by government. To ensure the integrity of information entered into the system, Oracle Financials is highly dependent on controls.

Common IT Services (CITS), a part of the Ministry of Management Services, has ownership and responsibility for the hardware and related operating software that CAS runs on. By connecting to the shared government network, ministry and agency staff can access Oracle Financials through a web browser, logging on with their unique government username and a password.

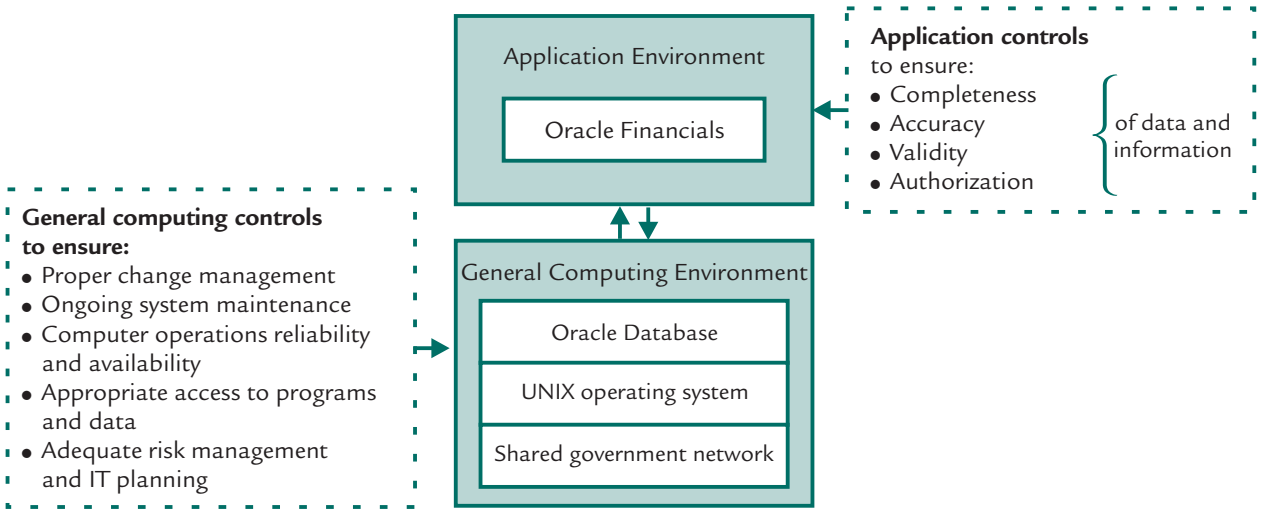
CITS and Corporate Accounting Services, also part of the Ministry of Management Services, work together to provide maintenance, security, capacity planning, back-up and recovery for Oracle Financials, the UNIX operating system and the Oracle database.

IT environment controls

As shown in Exhibit 2, the CAS computing environment can be conceptually divided into two main parts: the general computing environment (the Oracle database, UNIX operating system, and shared government network) and the application environment (Oracle Financials).

Exhibit 2

CAS computing environment



Background

The reliability of CAS depends on the controls over the general computing environment to ensure that the system is reliable, secure and available for processing. These controls include: segregation of incompatible duties, proper change management processes, appropriately restricted access to programs and data, performance monitoring, regular back-up and recovery, and adequate physical security.

The reliability of CAS also depends on having controls over the application environment to ensure that only authorized data is recorded and processed correctly. These controls include edit checks, exception and balancing reports, segregation of incompatible functions, and manual procedures performed by employees. They also include computer processes in the application that initiate, approve and match data, and ensure that data is correctly processed, posted and stored.

The adequacy of controls over the CAS general computing environment and the Oracle Financials application has a direct impact on the reliability and integrity of the accounting service across government and the government's financial statements. For this reason, a strong control environment must be in place. Such an environment requires a combination of both governance and system controls. Governance and system controls can be found in both the general computing environment and the application environment.

Governance controls are organizational and generally involve the development and implementation of policies, procedures and standards, followed by monitoring for compliance. *System controls* are programmed or manual techniques that appropriately restrict activities such as system maintenance, day-to-day computer operations, and access to data, programs and hardware, thereby ensuring the reliability, confidentiality and availability of system-generated information.

Governance controls can either enhance or reduce the effectiveness of system controls. For example, management can compensate for a system control deficiency by implementing a detective control such as monitoring. On the other hand, if management does not develop and enforce policies and procedures, such as those for issuing new usernames and granting levels of system access, system controls can be compromised.

Focus of our audit

The implementation and enhancement of the government-wide accounting and financial reporting system has been carried out by government in steps (see Exhibit 3). The CAS environment has continued to improve, with new functions and hardware added and existing hardware and software upgraded.

Our approach to examining CAS has involved several focused audits over three years. We have audited the UNIX operating system and the Oracle database and we have reviewed CAS's governance framework. Currently, we are auditing the controls directly related to purchase, accounts payable and general ledger transactions.

This is our first report and includes the work done on UNIX, the database and governance controls. A second report, to be issued this fall, will include any follow-up work required as a result of this report, as well as our assessments of purchase, accounts payable and general ledger controls.

We have not examined the controls over the transmission of information from the ministries to CAS (using the government shared network) or many ministry controls.

Audit criteria

Our audits of the UNIX environment and the Oracle database were based on criteria set out in the IT Control Guidelines issued by The Canadian Institute of Chartered Accountants. These guidelines provide standard control objectives used by Certified Information Systems Auditor specialists in Canada to carry out IT audit examinations. The objectives address the management of risks arising from the use of information technology, and the roles and accountabilities of the people who manage and use information technology.

Guidance from the IT Governance Institute formed the basis for our assessment of governance controls. The IT Governance Institute provides material to assist executives and boards in successfully meeting IT governance responsibilities. Methodology information was also obtained from other legislative audit offices in Canada.

Exhibit 3

History of the changes to the government's corporate accounting system

Year	Corporate Accounting System (CAS)							
	General ledger (GL)	**Accounts payable (AP) and purchases**	**Accounts receivable (AR)**	**Fixed assets**	**Data warehouse**	**Operating environment**	**Other**	**Office of the Auditor General audits**
1998	Oracle Financials pilot (implementation of GL, AP, purchase order modules for 2 pilot ministries)							
1999	Oracle Financials implementation of piloted modules for all ministries; transactions also entered into the old (Walker) system		Oracle Financials AR implemented for 1 ministry and 1 Crown corporation					
2000	Common chart of accounts implemented for all ministries				Data warehouse implemented for all ministries. (Minimal usage: still using old system.)			
2001	Walker system decommissioned; Oracle Financials now Corporate Accounting System			Oracle Financials fixed assets module pilot by 2 ministries	Data warehouse standard reporting for all ministries		Payment Review Office created	
2002	Treasury Board approval; Corporate Accounting System Initiative within $1,000 vote of Solutions BC	Oracle Financials iExpenses pilot (entry of travel expenses by employees) iExpenses implemented for all ministries		Oracle Financials fixed assets module implemented for all ministries				*Review of UNIX operating environment*

The CAS environment

Year	Corporate Accounting System (CAS)							
	General ledger (GL)	**Accounts payable (AP) and purchases**	**Accounts receivable (AR)**	**Fixed assets**	**Data warehouse**	**Operating environment**	**Other**	**Office of the Auditor General audits**
2003	New Budgeting and Chart of Accounts Maintenance implemented for all ministries	Oracle Financials iProcurement module pilot with 2 ministries		Fixed assets available to 21 organizations		Oracle Financials 11i upgrade provides technical foundation for future initiatives	Corporate Accounting System Initiative moved to Ministry of Management Services. Name changed to Corporate Accounting Services	*Audit of CAS Oracle database*
2004		Oracle Financials iProcurement implemented for all ministries					Single sign-on implemented for CAS Oracle Financials Self-service functionality for all ministries	*Review of CAS IT governance and follow-up on UNIX and database recommendations*
2005						Replacement and upgrade of CAS servers and UNIX operating system		

Source: Solutions BC Newsletter, Ministry of Management Services

It is important to note that any system of internal control has inherent limitations. This means that despite the control procedures in place, errors or irregularities may still occur and go undetected. Furthermore, evaluating a system's reliability in future periods is subject to the risk of procedures becoming inadequate as conditions change or of compliance with procedures deteriorating.

IT governance

Senior management has a process in place to ensure that the IT strategy for CAS is aligned with the government's business strategies and the CAS IT environment is managed in a way to ensure the continuous and effective delivery of service.

With the implementation of CAS, government has taken advantage of newer technology to provide an on-line, real-time central accounting system, with connection available through the Internet. The use of new technologies also introduces new risks to government. It is the responsibility of management to ensure the central accounting service provides good value and an acceptable level of risk. These responsibilities can be realized through successful IT governance.

IT governance is carried out through organizational controls that direct responsibility for IT planning, risk management and control, business continuation planning, and other activities that require centralized direction through policies, procedures and standards. These controls provide assurance that the use of IT is aligned with government's business strategies and that the IT environment itself is managed in a way that ensures the continuous and effective delivery of service.

Audit scope

The criteria we used for our assessment of these controls were based on guidance issued by the IT Governance Institute. Exhibit 4 lists the control areas that are relevant to the CAS IT environment and assigns responsibility for each area to either the corporate/program or activity level.

Who has corporate/program responsibility?

Strong IT governance is the responsibility of management at all levels—from the Director of Technology Operations to the Deputy Minister. Although Corporate Accounting Services has responsibility for CAS, as shown in Exhibit 5, the Office of the Comptroller General, the Government Chief Information Officer, Treasury Board, the Senior Financial Officers' Council and the Deputy Ministers' Council are also involved in determining the

Exhibit 4

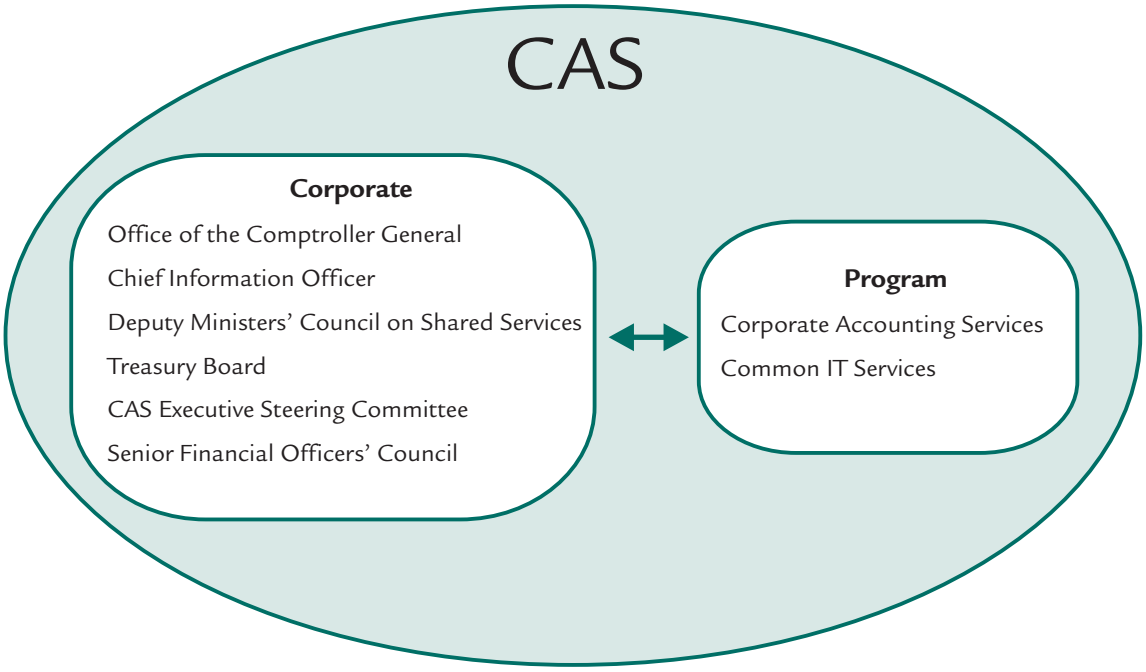
Assignment of control responsibility in the CAS IT environment

Control Area/sub-area	Responsibility Level	
	Corporate/Program	Activity
1. Planning and Organizing the IT Environment		
IT strategic planning	✓	
Information architecture	✓	
IT organization and relationship	✓	
Communication of management aims and direction	✓	
Management of human resources	✓	
Compliance with external requirements	✓	
Assessment of risks	✓	
Management of quality	✓	
2. Managing Changes to Programs and the System		
Develop and maintain policies and procedures		✓
Manage changes		✓
3. Delivering and Supporting IT		
Define and manage service levels		✓
Manage third party services		✓
Manage performance and capacity	✓	
Ensure systems security		✓
Educate and train users	✓	
Manage the configuration		✓
Manage problems and incidents		✓
Manage data		✓
Manage facilities	✓	
Manage operations		✓
4. Monitoring and Evaluating the IT Environment		
Monitoring	✓	
Adequacy of internal controls	✓	
Independent assurance	✓	
Internal audit	✓	

Source: *IT Control Objectives for Sarbanes-Oxley,* IT Governance Institute

Exhibit 5

Assignment of CAS corporate/program responsibilities



strategic direction of CAS. The CAS Executive Steering Committee, which functions as the representative owner, has overall responsibility for overseeing the scope, direction and priorities for CAS. Members of this committee include Assistant Deputy Ministers and Executive Directors from across government.

Common IT Services is responsible for controls over the servers, network and firewalls.

This section of the report focuses on our audit of corporate and program level controls. Activity level controls (operational controls such as managing day-to-day processing) are covered in later sections of this report on the UNIX operating environment and the Oracle database.

Conclusion

Management's aim is to efficiently use and manage available resources to achieve the government's goal—namely, that of providing one accounting service across government. In doing so, management is also responsible for establishing and maintaining adequate control.

We concluded that senior management has an adequate process in place to ensure that the IT strategy for CAS is aligned with the government's business strategies and to manage the CAS IT environment in a way that ensures the continuous and effective delivery of service.

Management has appropriately set the objectives, established the policies and made the decisions that direct the planning and the organization of the CAS IT environment, the delivery and support of IT, and the monitoring and the evaluation of IT. Several areas where improvements could be made have been noted.

Planning and organizing the CAS IT environment

Because CAS is a complex environment with many stakeholders across government, IT governance involves communication and direction from many interest groups. This requires the interaction of numerous committees, each with representatives from various levels of government.

We found appropriate governance over planning and organizing the CAS IT environment. Senior management direct and are appropriately involved in IT strategic planning, establishing policies and procedures, and communicating their direction through these established policies and procedures.

IT strategic plans are now in place for Corporate Accounting Services and at the ministry level. Although an IT plan for Corporate Accounting Services was established, it was not clearly integrated with its business plan or in the ministry's overall IT strategic plan for fiscal 2004/2005. Procedures are now performed to integrate the Corporate Accounting Services IT plan with its business plan and the ministry's IT strategic plan.

IT governance

Corporate Accounting Services gives appropriate attention to the identification, assessment and management of information technology risk and uses a number of different risk management processes and tools.

A culture of management integrity, including business practices and ethics, and human resources evaluation has been adopted and promoted by Corporate Accounting Services. Policies and procedures are in place to ensure that security and technical issues are considered when staff are hired, retained or terminated. Corporate Accounting Services promotes continuous learning and provides the necessary skill development to staff.

The organizational structure at Corporate Accounting Services allows for a proper segregation of incompatible duties. Organization charts show management oversight relationships and the responsibilities of each team. Job descriptions communicate the roles and responsibilities for each team member. These tools are important to ensure there is a proper segregation of duties and that a suitable number of employees with appropriate skill sets are maintained.

Standards for how data is captured, processed and reported, ensuring its quality and integrity, and standards on classification, filing, retrieval and disposition of both electronic and paper records are outlined in the government's Core Policy and Procedures Manual. As well, Corporate Accounting Services has processes to ensure compliance with legal, regulatory and other contractual requirements.

We believe that Corporate Accounting Services could further improve governance in the area of planning and organizing of the IT environment by addressing the following deficiencies.

1. Given the significant changes in the organizational structure of government and at Corporate Accounting Services during the last few years, we found that some of the job descriptions needed to be updated to reflect the current structure at Corporate Accounting Services.

   We recommend that job descriptions be reviewed regularly to make sure that the roles and responsibilities are still current and the skills and experience required are clearly specified.

2. Although policies and procedures governing activities related to CAS are developed, documented and communicated by management, we observed that some of these documents are labelled as "draft" and may not represent current and accurate information.

   We recommend that policies and procedures be regularly reviewed and updated in order to provide current and accurate information to users. A history should be maintained to inform users of the changes and the current approved version in use.

   We also recommend that a process be in place to monitor compliance with policies and standards.

3. A Business Continuation Plan (BCP) exists and tests have been conducted to ensure the availability of information and services in the event of disruption. The last tests were performed in December 2003. The government's Core Policy and Procedures Manual requires such tests to be performed annually. However, because of planned changes to the operating system, annual tests were not performed in December 2004.

   We found that the BCP does not have detailed wrap-up procedures, and the corresponding "quick reference" guide is missing sections and contains incorrect section references. The next updated version of the plan is scheduled for spring 2005, after changes have been made to the operating system. As well, the last risk assessment for BCP purposes was done in August 2002 and now likely contains outdated information because of changes in CAS operations since then. As CAS is a significant government system, this assessment should be performed.

   We recommend that a Business Continuation Plan risk analysis and testing be performed annually (or when significant changes occur) and that the plan be updated regularly to ensure its contents are complete and accurate.

4. There are quality management standards and systems at Corporate Accounting Services. However, we found evidence that important documents such as quality management plans were not always prepared for projects.

We recommend that a quality management plan, defining the quality assurance process and how it will be implemented, be prepared for each project as required by the adopted standards.

Delivering and supporting CAS IT

Corporate Accounting Services has processes in place to measure system performance and monitor capacity issues. Computer facilities are sufficiently managed.

A process is in place for identifying the training needs of all users in support of the long-range plan. Management also provides education and ongoing training programs that discuss ethical conduct, system security practices, confidentiality standards, integrity standards and security responsibilities of all staff.

Operations performance is monitored on a daily, weekly and monthly basis by Corporate Accounting Services. However, there is no process in place to regularly monitor the overall actual performance in relation to the capacity and technology plan. Governance in this area could be improved by addressing this deficiency.

To detect potential capacity concerns, **we recommend that a process be in place to monitor overall information technology performance by comparing actual performance to the capacity and technology plan on a regular basis.**

Monitoring and evaluating the CAS IT environment

Senior management at Corporate Accounting Services monitors and evaluates the CAS IT environment by using benchmarks, such as CAS availability measured in hours per week. Internal control assessments are periodically performed by Internal Audit and Advisory Services in the Office of the Comptroller General, to examine whether internal controls are operating as they should.

Corporate Accounting Services participates in the current benchmarking initiative of the Ministry of Management Services, using the Hackett Group, an external consulting firm specializing in benchmarking. There are other benchmarking measures that could also be researched and used, such as Oracle Application's standard benchmarks or those outlined by other consulting groups, such as Forrester Research Inc.

UNIX operating system

At the time of our follow-up, we identified several control issues that could result in unauthorized access to the system or government information. Significant changes being made to the environment will require a further follow-up assessment.

The Oracle Financials application and Oracle database run on a UNIX operating system, on computer hardware physically located in Victoria. Assessing controls in UNIX was our first step in evaluating the overall CAS computing environment.

Audit scope

Assessment criteria for the UNIX environment were based on the *Information Technology Control Guidelines* of the Canadian Institute of Chartered Accountants. Our review was designed to establish whether any of the following risks existed in the CAS UNIX environment:

- The operating system can fail to meet or keep up with future business objectives, thereby affecting performance or availability;
- Unauthorized changes can be made to the operating system, thereby affecting security, availability or performance;
- Unauthorized access to view or change government data can occur through access obtained through the operating system, resulting in a loss of data integrity or data confidentiality; or
- The physical environment can be compromised by unauthorized access or a disaster, leading to system unavailability or loss of data integrity and confidentiality.

The control objectives addressed in this review are outlined in the sidebar.

We examined the UNIX operating system running on the five production servers housing the Oracle Financials application, database and back-up. Each server was electronically scanned using a commercially available security assessment tool and potential issues identified by the scan were investigated. The scans were designed to identify security exposures and vulnerabilities from five sources: external attacks, super users (those with advanced access or special privileges on the system), ordinary users, files and devices, and system files.

UNIX Operating System Control Objectives

The control objectives should be designed to ensure:

- the UNIX operating system continues to meet business and technical requirements;
- operations services are appropriately controlled and meet defined user requirements efficiently and effectively;
- the integrity and availability of computer operations services are maintained;
- systems software procedures and activities contribute to the reliability, effectiveness and control of computer operations services;
- appropriate controls are established over information transmitted to and from outside organizations;
- the integrity, confidentiality and availability of information technology processing are maintained;
- access to the UNIX operating system and information is reliably controlled;
- appropriate consideration is given to security issues and technical skills when management and staff are hired into information technology positions;
- information technology security is operated in an efficient and effective manner; and
- critical information systems processing functions can continue, or be resumed promptly, in the event of significant disruption to normal computer operations (information technology recovery planning).

Conclusion

Our review focused on the state of the system in the spring of 2002. Although potential issues and risks were found and investigated, we noted that other controls existed that partially mitigated these risks. Weaknesses noted during the review are outlined in Exhibit 6. However, given the compensating controls identified, we concluded that the control environment satisfied all control objectives.

During our audit of the CAS Oracle database in the fall of 2003, we re-examined certain areas of the UNIX operating system: access from the UNIX operating system to the database, controls around UNIX usernames and passwords, and certain controls in the network (particularly the firewall). We identified several control issues in this audit that could result in unauthorized access to the system or to government information. (We discuss these further in the next section of this report.)

Exhibit 6

Recommendations from our original review, to be re-evaluated and followed up after the planned upgrades to the operating system are completed

Area/Issue	Description	Risk Level
Security		
UNIX security checklist was out of date.	Security settings suggested by the current security checklist may not address recent security vulnerabilities. The current checklists do not reflect the actual current system configuration. **We recommended to CITS that the UNIX security checklist be updated to reflect checks for current known vulnerabilities, and be updated for the current system configuration.**	Medium
UNIX systems were not scanned for known vulnerabilities on a regular basis.	The UNIX systems owned and administered by CITS, are scanned for known system vulnerabilities. However, various non-commercial utilities and scripts are used and the scanning is not performed on a regular basis. If scanning is not performed on a regular basis using a tool with a current vulnerabilities definition, there is a risk of CAS systems being exposed via newly discovered operating system security vulnerabilities. **We recommended that a systematic, scheduled process for regular scanning of all UNIX systems for known vulnerabilities, using a commercial tool, be implemented. The scanning tool should be regularly updated to include checks for up-to-date known vulnerabilities.**	Medium
Remote login was insecure	Due to the nature of TELNET and FTP protocols, their communication mechanism is not encrypted and it is possible to observe full and unencrypted communication using a network sniffer utility. TELNET and FTP protocols are not encrypted even during a process of user authentication and thus it would be possible to find out the passwords of individual users. See recommendations in the Oracle database review (next section of this report).	
Business Continuation Planning		
Business Continuation Plan was not recently tested	Regular testing of a Business Continuation Plan is needed to assess its viability and to identify any missing components. Recovery capability cannot be completely demonstrated until all components of the plan are tested. In addition, it is likely that some of the procedures tested are no longer relevant as a result of reorganizations, changes in infrastructure, and hardware and software updates. **We recommended the complete restoration of the system environment be thoroughly tested on a regular basis (for example, once per year).**	Medium

Unix operating system

We have not followed up on the issues presented in Exhibit 6, since, between September 2004 and January 2005, all CAS servers were being replaced or upgraded and the UNIX operating system upgraded. Data storage capabilities were also being increased (because storage requirements have grown significantly as a result of the retention of historical and other data). These upgrades will result in significant changes in the operating environment and will require a follow-up assessment. We will report on our assessment later this year.

Oracle database

Many of the necessary controls over the Oracle database were in place. Additional controls should be implemented to ensure information stored in the Oracle database used by CAS is secure and can be relied on.

All transactions entered in Oracle Financials are recorded in the Oracle database. From this, management develops budgets and generates information for both decision-making and financial reporting. Most importantly, these database records are used to generate payments and to produce the government's financial statements. If controls restricting inappropriate access to database records are not effective, these records could be altered or deleted, resulting in incorrect payments or inaccurate financial statements.

Audit scope

We conducted our work using the control objectives outlined in the *Information Technology Control Guidelines* of The Canadian Institute of Chartered Accountants.

We identified the control objectives relevant to the Oracle database (see sidebar) and, for each control objective, identified a number of procedures that would ensure the objective was being met. We performed our assessment of these control procedures from April to September 2003.

Oracle Database Control Objectives

Control objectives should be designed to ensure:

- there is proper management over authorized changes or additions to the components of the database infrastructure;
- the database is protected against accidental or unauthorized changes;
- the database production environment is appropriately controlled and meets defined user requirements;
- all Oracle processes and users are authorized and authenticated to the database and that user processes are controlled;
- IT security is operated in an efficient and effective manner;
- logical access to the Oracle database is reliably controlled;
- appropriate consideration is given to technical skills when management and staff are hired for IT positions, and to security issues when management and staff are hired or terminated; and
- the database is available for users, and processes and appropriate measures have been taken to limit the exposure of component (hardware) failure, media failure or other system or business interruption.

Conclusion

Many of the necessary controls over the Oracle database were in place. However, we did identify some control deficiencies that could jeopardize the integrity and reliability of the information stored in the database. We made several recommendations to improve the management and control of the database. In November 2004, we assessed the status of our recommendations. Following is a description of the control deficiencies we noted at the time of our audit, along with the status of recommendations made to improve controls.

Managing the database

To evaluate the management of the Oracle database, we examined controls such as monitoring service levels, identifying and registering hardware and software, managing licence agreements, capacity planning, controlling system changes and exercising problem management. We found that:

- there was appropriate monitoring of service levels;
- change control processes were in place and followed;
- problem management processes were operating effectively; and
- capacity planning was in place, although changes could be made to improve its accuracy.

We also identified the following key deficiencies.

The licences for direct access to the database, rather than through Oracle Financials, are handled using a "named-user" licensing scheme. Named-user licences are required for those staff that have direct access to the database for development and maintenance, and are managed by Common IT Services (CITS), based on information supplied by Corporate Accounting Services. At the time of our audit, Corporate Accounting Services was unable to determine whether the appropriate number of Oracle database licences were issued. CITS keeps a list of developers that require named-user licences, but our review of the list revealed that it was out of date. This could result in a significant over—or under—payment for licensing and we recommended that a framework be developed for managing licences. During our follow-up, we noted that Corporate Accounting Services has

developed such a framework and conducted a comprehensive review of licensing. We agreed with the conclusion of that review, which found that Corporate Accounting Services was in compliance with the Oracle vendor licensing rules.

During 2003, management responsibility for the CAS servers was transferred to CITS. At the time of our audit, CITS did not have a system in place to track product information about the CAS servers and other CAS hardware components. Without such a system, management cannot know if hardware costs being paid by the government to replace defective components are actually covered under warranty. We recommended that Corporate Accounting Services ensure the complete, accurate and timely recording of all CAS hardware. Since our audit, that has been done.

Effectiveness of controls over the database

To measure the effectiveness of controls that ensure the security, availability, reliability and integrity of the Oracle database, we looked at controls at the database, host operating system and network levels. These controls included:

- logical access (access to the system using unique usernames and passwords that have been mapped into pre-defined levels of access) granted to users of the Oracle database and UNIX operating system;
- the administration of usernames and passwords;
- capturing and logging specific high risk access activity for monitoring and audit trail purposes;
- back-up procedures;
- disaster recovery procedures;
- the use of encryption processes that take original data, translates it into an unrecognizable format for transmission over the network, and then returns it to its original form; and
- firewall controls.

We found that many of these controls were in place and functioning properly at the time of our audit. However, we did find four key deficiencies.

First deficiency: changes to database tables

At Corporate Accounting Services, database administrators have access to all data in all tables. This is needed for business operations, but it introduces the risk that unauthorized changes could be made. A detective control, such as auditing system and database administrator activities that involve high-risk data (including bank account information and usernames and passwords) would reduce these risks, especially where it is not possible to have an appropriate segregation of duties.

At the time of our audit, Corporate Accounting Services had not activated the auditing function for Oracle Financials. If auditing were activated, the audit log would show who made changes to the data and when and could be analyzed for appropriateness. This is not a foolproof solution however, since the audit records can be deleted from the audit log by users with the database administrator role or users who are able to enter the Oracle database from the UNIX operating system. Therefore, a method must also be implemented that prevents users from turning off auditing or gaining access that allows them to change the audit log.

Logging information on activities that involve high-risk data is only the first step. It is also important that someone that is not involved in operational activities be assigned to review the audit logs regularly and follow up on any unusual activities.

We recommend that Corporate Accounting Services identify high-risk information in the Oracle database, implement an audit log—that cannot be altered—that records changes made to this information and assign an individual to review the audit logs regularly and follow up on any unusual activity.

During our follow-up work, Corporate Accounting Services informed us that an Enterprise Security Officer position has been created. The role of this position is still being developed but will include the responsibility for identifying the high-risk data and database tables that should be audited. It is anticipated that the position will be filled in the spring 2005.

Second deficiency: database access

Access to the Oracle database can be achieved through either the UNIX operating system or using usernames and passwords.

Access through the UNIX operating system

A person who has certain access to the operating system could use a tool to gain full access to the Oracle database. This means they could access and change all data and user assigned privileges and alter table structures through the data dictionary, a list describing and defining all data in the database.

We found that CITS computer support staff, the database administrators, and some CAS specialized support staff have these powerful access privileges. The tools that allow this access are required by most of these support staff for other reasons, but could also be used to gain full access to the database. Since there are business reasons for the use of the tools, gaining access to the database by this means cannot be prevented.

Accesses gained this way are logged, but the logs are not reviewed or analyzed. To compensate for the security risk introduced by the tools, we recommended that the log that records this method of database entry be reviewed on a regular basis.

During our follow-up, we verified that the log recording the database connections made using these tools is now reviewed daily by an appropriate staff member. All connections are reviewed and discrepancies are brought to the attention of Corporate Accounting Services management. We also verified that access to the tools by those CAS support staff not requiring it has been removed.

At the time of our audit we found that, because of both the unmonitored access gained through the UNIX operating system and the absence of auditing access logs, some data tables that would generally be evaluated as properly secured were in fact at risk of undetected access. That is, they could be changed or deleted without any trace of activity in the system. This included all data within tables, including those containing usernames and passwords, assignment privileges to users, and high risk data such as bank account information.

Corporate Accounting Services can reduce this risk by implementing the recommendations relating to the audit of changes to high-risk data, and by monitoring the corresponding audit logs and accesses through the UNIX operating system.

Access to the scripts (programming code in the system) containing usernames and passwords, should also be restricted. Some CITS support staff have read-only access to most scripts. Therefore, if passwords were contained in any of the scripts, those staff would have access to them. Since there is no apparent way to prevent CITS support staff from learning the application passwords, the risks could be reduced by implementing the recommended auditing process.

Access through usernames and passwords

Default Usernames and Passwords – As is common for many commercial software packages, the Oracle vendor supplies default usernames and passwords that are intended for use by database administrators, Oracle applications and Oracle processes when the application is initially loaded onto the operating system and run. The default usernames are configured in the application with default passwords that are not preset to expire and be renamed after a specified short period. Therefore, unless default usernames are required for testing or other purposes, they should be disabled before the Oracle database is placed into production. Upon installation, passwords for all default usernames that are required should be changed immediately.

At the time of our audit, we noted that one of the default usernames was still set to the default password. This occurred because Corporate Accounting Services had installed a patch approximately six months earlier that set the password back to the default. This means that an external hacker, or an internal user, might be able to penetrate the network and thus gain access to a username and password that has privileges on the production database by just entering the default values. The database administrator who found this default password during our audit, changed it immediately.

We also noted that an Excel spreadsheet is used to record the passwords of the default usernames. When these passwords are changed, updates are made in the spreadsheet, which is password-

protected and stored on the Corporate Accounting Services network. The password for the spreadsheet is only known by the database administrators and some specific technical staff. The password does not expire, but it is changed regularly and immediately if someone with knowledge of it leaves their position. To further protect the information in this spreadsheet, we recommended that access be appropriately restricted to the network directory where the spread-sheet is stored.

During our follow-up, we verified that the network directory containing the password file is now restricted appropriately. The password protecting the network password file is being changed when a database administrator or support person with knowledge of the password leaves their position.

Database Administrator and Oracle Application Usernames and Passwords – As noted earlier, anyone can gain direct access to the Oracle database by having a username and password with which to log on. We found that direct access to the database was appropriately restricted to database administrators only.

The database administrators at Corporate Accounting Services change the passwords for the two administrator accounts whenever someone leaves the position or a security exposure is suspected from the passwords being compromised. The same password is used for both accounts. The passwords for the Oracle Financials application accounts are changed manually at the same time as the passwords for the two Oracle database administrator accounts. The passwords for these usernames are set to different values in the development, test and production environments. Only the database administrator staff and limited CAS technical support staff know the passwords. The Information Technology Security Policy, maintained by the Office of the Chief Information Officer, recommends that password expiration time be set based on the sensitivity of the data to be accessed.

We recommended that Corporate Accounting Services and CITS review their password expiration policy and change passwords based on the risk of exposure to the data if passwords were compromised. During our follow-up, we found that password expiration has now been standardized according to policy.

Oracle database

At the time of our audit, UNIX passwords used by Oracle processes and CITS support staff were set to the same password on development, test, production, training and disaster recovery servers. A password exposure on any of the servers could therefore also result in an exposure on the production server.

We recommend that the passwords used on the production servers be set to different passwords from those in the test and development environments.

We also found several instances where the levels of access granted exceeded what was needed for business purposes. During our follow-up, we noted that our recommendations had been followed and the access was eliminated.

Third deficiency: database networking

To connect to the Oracle database, the user must communicate with an Oracle product called the "Listener," which runs on the server machine. Since the Listener service is essential for communication with the database, it should have the necessary safeguards to ensure its availability.

We recommended that the Listener service be password-protected to prevent an unauthorized command being issued that could interrupt the service. During our follow-up, we verified that password protection has been added.

Firewall access

> **What is a firewall?**
>
> A firewall is a system designed to prevent unauthorized access to or from a private network. It can be hardware, or software or a combination of both. All messages entering or leaving the internal network pass through the firewall, which examines each message and blocks those that do not meet specified security criteria.
>
> Source: Webopedia at www.pcwebopedia.com

Software firewalls are installed on each CAS server to protect the servers from unauthorized external access. The firewall rules are managed by Corporate Accounting Services and implemented by CITS. Access to and from the servers is either permitted or prevented, depending on the specific ranges of IP addresses.

Each of the servers is synchronized with the same set of firewall rules. The rules currently permit all the shared government network users access to the test and development servers. These should only be accessed by support staff and other CAS servers.

We recommend restricting access to the test and development servers to only those IP addresses that require access.

What is an IP address?

An IP, or Internet Protocol, specifies the format of packets and the addressing scheme. Most networks combine IP with a higher- level protocol called a Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and source.

An IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. A TCP-IP combination, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

Source: Webopedia at www.pcwebopedia.com

What is a FTP?

A FTP, or File Transfer Protocol, is used for exchanging files over the Internet.

Source: Webopedia at www.pcwebopedia.com

What is a Port?

A port is used to designate user access to features or software on a host server. Just as a ship entering the harbour, the user has to know at what port it will dock (connect to). Common TCP-UCP "Ports of Call" are:

20 FTP (file transfer protocol data)

23 TELENET (terminal emulation

Source: TECHtionary at www.techtionary.com

At the time of our audit, we supplied CITS Network Services with a list of all the shared government network IP address ranges that were defined in the CAS IP filter file. We determined that access through the firewalls well exceeded the required and intended access to the CAS servers. Many schools, private businesses, wireless connections and undefined addresses were allowed through the firewall.

We recommend determining the appropriate IP addresses for access to CAS and restricting the firewall rules accordingly.

As Corporate Accounting Services is responsible for ensuring the firewall rules are correct, we previously recommended that they approve any changes to the rules prior to implementation. At the time of our follow-up, Corporate Accounting Services told us that there is now a formalized process in place to ensure that only approved changes are implemented.

The availability of FTP services on CAS servers adds two more risks to the computing environment. First, it opens the FTP port up to outside access and therefore the possibility of an attack. And second, because all data transfers are in clear text, and not encrypted, usernames and passwords could potentially be retrieved by a hacker monitoring the line.

At the time of our audit, the FTP service was needed to enable data transfer from the database server to the mainframe environment at CITS, and to support the Integrated Chart of Accounts and Budget Module (ICBM). The ICBM was replaced in October 2003. Currently, the only FTP need is for file transfers between the Oracle database server and the mainframe environment.

Data transfers between the database server and the mainframe using the FTP service are sent in clear text across the network. The transfers are sent only on the network within the computing facility and never go out to the public network. Therefore, if an exposure of the data occurred while in transport, it would be either from someone gaining access to one of the three routers situated between the CAS servers and the mainframe or from a "sniffer" within the facility. (A sniffer is a device that monitors data travelling over the network.)

What is TELNET?

TELNET is a terminal emulation program for TCP-IP networks such as the Internet. The TELNET program runs on your computer and connects you to a server on the network. You can then enter commands through the TELNET program and they will be executed as if you were entering them directly on the server console.

Source: Webopedia at www.pcwebopedia.com

Since the FTP service is required just on the Oracle production database server, we recommend adding a rule to the IP filter that allows only the mainframe IP addresses to use the FTP port on the production database server and disables the service on the other servers.

TELNET services are also available on all CAS servers. The same security issues are present with TELNET as with FTP. However, Corporate Accounting Services has implemented some safeguards around the availability and the use of TELNET services. The risk still exists that when the TELNET port is open, there is potential for an outside attack in the event the firewall monitoring is interrupted. However, there are port restrictions in the firewall rules that limit the service. TELNET transfers data across the network in clear text, but firewall rules require TELNET be used with a virtual private network (VPN) to access the servers. Therefore, clear text transport is not permitted through the firewall.

What is a VPN?

A VPN, or virtual private network, is a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Source: Webopedia at www.pcwebopedia.com

The TELNET service is used by some system processes and by support staff for resetting remote user passwords. Every six months, the need for TELNET is reviewed. To date, the need for TELNET still exists, but is not required on all servers.

We recommend adding a rule to the IP filter that only allows the TELNET port to be used on the servers that require TELNET.

All CAS users with usernames on the Oracle database server—for example, CAS developers, business analysts, database administrators, and some CAS and CITS support staff—are able to connect remotely to the database from their home computers. Traffic from remote computers via the VPN gateway service ensures that all data is encrypted. When this type of connection is permitted, the organization must enforce virus protection policies to ensure that a home computer does not send a virus to the CAS servers and that there are no malicious programs, such as Trojan horses, on the home computers. Some of these programs can record a user's keystrokes and send the information to a hacker, including the user's username and password.

Firewall failure

The firewall rules are designed to prevent unauthorized external access. Conditions such as accidental changes to firewall rules, which create partial security threats from the outside, or malfunctioning firewalls, which leave no protection, have occurred in the past, resulting in CAS servers being used for third-party mail relay, that is e-mail was sent out that looked like it originated from the CAS server.

We became aware of one instance where third-party mail relays occurred because the firewall was not running. It was 15 hours after the firewall went down before CAS support staff noticed that no entries were being made to a log.

Support staff are paged when port scanning occurs (since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer), but there is no process that pages staff when the firewall is not functioning. The firewall is integrated into the UNIX operating system at the network layer, and therefore cannot go down without the operating system going down. If the firewall does not come up with the server, as was the case here, all connections would be able to get to the server.

The firewall could be running, but—because of an error in the firewall rules—unauthorized traffic could be allowed in. This situation happened during the course of the audit and resulted in a third-party spam mail relay. According to the report on this incident, the situation was due to human error and non-compliance to CITS change management process.

CITS support staff are currently not notified when the firewall is not running. According to support staff, this service could be provided through development of an in-house system that would page staff when the firewall is not running.

We recommend that a process be developed to immediately notify support staff when the firewall is not running. This would address the exposure if the firewall was not brought up with the system.

We recommend that Corporate Accounting Services and CITS review the current firewall single-point of failure configuration to determine if a more secure configuration can be devised.

At the time of our follow up, the firewall rules were in the process of being revised. We will report on our assessment of these changes later this year.

Fourth deficiency: database availability, back-up and recovery

To ensure that the Oracle database is available for users and processes, appropriate measures must be taken to limit exposures due to system failure. Two important methods to achieve this are the development and testing of a disaster recovery plan and a business continuation plan.

The CAS Business Continuation Plan indicates that earthquakes are commonplace in British Columbia. It lists two main earthquake threats ranging from 7 to 9.2 on the Richter scale. Back-up and offsite storage of the data and application are located in Victoria and Vancouver.

Alternate back-up sites outside the active seismic zone have been considered but not implemented because of funding issues. Because the back-up and offsite facilities are both in the same geographical location, there is a potential for the loss of data if a major earthquake occurred.

We recommended that Corporate Accounting Services consider having storage outside the active seismic zone for tapes containing programs and data. During our follow-up, we were informed that an investigation performed by Corporate Accounting Services found that relocation of the storage outside the seismic zone was not feasible. However, with recent changes, in Kelowna and Kamloops, they have asked CITS to review the feasiblity of relocating to one of those locations.

Response from the Ministry of Management Services

The Corporate Accounting Services Office is pleased to respond, on behalf of the Ministry of Management Services, to the Auditor General's findings in the report "Audit of the Government's Corporate Accounting System: Part 1."

Firstly, I would like to thank the audit team for their comprehensive work on this review and the positive feedback and recommendations we have received from them on the governments financial Corporate Accounting System (CAS).

CAS is an integrated Oracle based financial system that includes the following core modules Accounts Payable, i-Procurement (purchasing), i-Expense (travel), Purchase Order, Fixed Assets, Accounts Receivable, and General Ledger. Corporate Accounting Services is the owner of CAS and is responsible for ensuring the system meets the needs of it's clients and also meets the governance standards, legislation and policies of the governing bodies such as the Office of the Comptroller General (OCG), Common Information Technology Services (CITS), and Treasury Board.

Corporate Accounting Services works closely and in collaboration with the above groups to ensure that we meet or exceed the standards required, in this ever changing environment, and were please that the Auditor General identified in the report that he, "found the control environment examined for this report to be well managed." We are also pleased to identify that there have been no known security breaches in the CAS environment.

The Auditor General has provided in his report some recommendations that would further improve the control environment around CAS many of which have now been implemented by, Corporate Accounting Services, or are in process. This includes: better integration of the Corporate Accounting Services IT plan with the ministry overall IT plan; through working with CITS, we have further strengthened the control environment around the UNIX system; addressing database control issues by turning on the 'audit' function in the application; creating a new Enterprise Security Officer position; upgrading the server hardware; and, working with CITS to improve existing firewall rules and access via SPAN BC.

As well, it is important to note that CITS is currently undertaking a Security Enhancement Project. The primary objectives of the Security Enhancement Project are:

- *To clarify and strengthen the government's policies, standards and guidelines respecting IM/IT security;*
- *To reduce current vulnerabilities to unauthorized access to information;*
- *To prevent the disruption of the government's critical infrastructure and business;*
- *To minimize damage and the recovery time related to disruptions that do occur; and*
- *Identify future requirements for security enhancements as new technology is adopted and security threats/risks are identified.*

Other projects underway in Corporate Accounting Services to address recommendations include:

- *Review and update of relevant job descriptions – now underway with expected completion in fiscal 2005/06;*
- *Continued review of internal Corporate Accounting Services policy and procedure documentation and standards - ongoing;*
- *Upgrade of Disaster Recovery server hardware – expected to be completed in September 2005*
- *Working with CITS to address IP filter rules – currently under way*
- *Working with CITS to identify the feasibility of moving information storage facilities outside the seismic zone.*

Response to recommendations

IT governance

Planning and organizing the CAS IT environment

- **Regularly review and update policies and procedures in order to provide current and accurate information to users. A history should be maintained to inform users of the changes and the current approved version in use.**

  Corporate Accounting Services (the CAS office) will continue to review and update it's internal policies and procedures and will incorporate a versioning section in the documents.

- **Develop a process to monitor compliance with policies and standards.**

  As part of every development or operational project the CAS office ensures that the relevant government financial and management policies and procedures are met. The CAS office is further improving its existing Quality Review Process with additional formal, pre-defined criteria to evaluate project deliverables. These criteria will be finalized over the next six months and will strengthen adherence to applicable internal and government wide policies and standards.

  The CAS office will review its current process to look for further improvements.

- **Regularly review job descriptions to make sure that the roles and responsibilities are still current and the skills and experience required are clearly specified.**

  With the ever-changing environment that the CAS office works in, there is a need to ensure job descriptions are current. The CAS Office includes a human resource focus in it's business plan and also plans on completing a high level review of all job descriptions this fiscal year.

- **Perform a Business Continuation Plan risk analysis and testing annually (or when significant changes occur) and update the plan regularly to ensure its contents are complete and accurate.**

  The CAS Office updates and tests the BCP on a yearly basis. The plan was last tested in December 2003. The CAS Office made a business decision to delay the testing for 2004 due to their significant

hardware replacement from September 2004 to September 2005. Annual tests are recommencing in October for Disaster Recovery exercises.

The CAS office prepared a design of the existing BCP for its clients and several new options for expansion. This was presented at, and an option approved by, the Senior Financial Officer Council and the CAS Executive Steering Committee.

To further address this recommendation the CAS Office has created a Business Continuation Advisor position on staff.

- **Prepare a quality management plan, defining the quality assurance process and how it will be implemented, for each system project as required by the adopted standards.**

The CAS office has been working to meet this recommendation since it was first brought forward.

Over the last four months CAS has been developing an overall CAS Quality Management Framework, which will document the repeatable processes and procedures used to manage quality on all CAS Office projects.

Presently the CAS Office conducts quality planning for every project using the pre-defined series of "Quality Checkpoints" for significant deliverables as defined in the CAS Office Systems Development Lifecycle documentation. Quality activities are planned at the beginning of each project. Procedures are being developed to provide guidance to staff on the type and amount of quality management detail required on any specific project.

In the fall of 2004, CAS created a new position entitled the Manager of Performance and Risk Management. This position is responsible for establishing quality management standards in CAS. A cross-functional committee has also been established to serve as a focal point for quality improvement initiatives.

Delivering and supporting CAS IT

- **Develop a process to monitor overall information technology performance by comparing actual performance to the capacity and technology plan on a regular basis.**

*The CAS Office infrastructure environment is sized to handle the maximum load experienced by the application and the respective servers, which is fiscal year end. It is important to note that this **maximum** load only occurs **once** a year as a result of the significant number of fiscal year end transactions. The CAS Office has carefully planned its sizing around this important factor along with consideration of several other important inputs (such as project impacts, etc.). As such we do a realistic capacity plan comparison and review at that time. Once the performance numbers are collected they are compared against the capacity plan, which is then adjusted accordingly.*

The Capacity and Technology Plan is used throughout the year not just at fiscal year end. Each time a project or significant activity is identified at the CAS Office, the Project Initiation Document (PID) must include any impacts to capacity. If impacts are identified, the Technology Operations group assesses the Capacity and Technology Plan and makes any necessary adjustments.

As a note, CAS engaged independent 3rd party experts to complete the plan, in collaboration with CITS and the CAS Office technical staff.

The CAS Office will review our current process for monitoring capacity and performance to seek improvements.

UNIX operating system

- **Set the passwords for the production servers to different passwords from those in the test and development environments.**

The CAS Office will incorporate this recommendation.

Oracle database

Effectiveness of controls over the database

- **Identify high-risk information in the Oracle database, implement an audit log—that cannot be altered—that records changes made to this information and assign an individual to review the audit logs regularly and follow up on any unusual activity.**

As a result of the audit, the CAS Office has taken several positive steps to strengthen its existing security structure including turning on 'auditing' for the application and monitoring the database on a daily basis. The Data warehouse 'audit' feature has been on in DW production since March 2004.

The CAS Office is in the process of identifying methods for protecting the audit log and will also discuss options with the vendor.

A new Enterprise Security Officer (ESO) position was created, in January 2005, to review staff roles, monitor the audit log and to maintain a security framework within the CAS Office.

The ESO is actively reviewing known high-risk tables and is working to identify additional tables for review.

The ESO follows up on all unusual activity and looks for and reviews any attempts to access the database.

Firewall access

- **Restrict access to the test and development servers to only those IP addresses that require access.**

As a result of the firewall recommendations, the CAS Office is actively working with CITS to improve the existing CITS firewall rules and access via SPAN BC. Although the CAS Office owns the applications and therefore the business requirements; CITS owns the servers and must provide the business solution, therefore, the firewalls are a shared responsibility and solutions or changes are generally a result of a team effort. CITS is currently in the process of reviewing new firewall options and service offerings.

- **Determine the appropriate IP addresses for access to CAS and restrict the firewall rules accordingly.**

  As a result of the audit the CAS Office, with the assistance of CITs Network Services, has narrowed the IP subnets allowed through the CAS firewall down to specific IP ranges. These are further restricted to the higher network ports to allow application access and are blocked on all privileged ports. Access to non-government addresses is blocked both at the Internal Gateway and on each CAS server.

  The CAS Office is reviewing the impacts of implementing the recommendation. The CAS office continues to work with CITS to further improve and establish an acceptable balance between control and risk.

- **Add a rule to the IP filter that allows only the mainframe IP addresses to use the FTP port on the database server and disables the service on the other servers.**

  The CAS Office is actively working on this issue with CITS and Telus.

- **Add a rule to the IP filter that allows only the TELNET port to be used on the servers that require TELNET.**

  As a result of the audit the ports relating to TELNET and FTP are treated as privileged and access is restricted. The CAS Office will continue to review the requirements.

- **Develop a process to notify support staff when the firewall is not running.**

  The CAS Office is working on this issue with CITS.

- **Review, along with Common IT Services, the current firewall single-point of failure configuration to determine if a more secure configuration can be devised.**

The CAS Office is actively working on this issue with CITS. Firewall rules are also on the network gateway in addition to the CAS servers. This was implemented last fall in response to the firewall incident.

Appendices

Appendix A

Summary of Recommendations

We recommend that Corporate Accounting Services:

IT governance

- **Regularly review and update policies and procedures in order to provide current and accurate information to users. A history should be maintained to inform users of the changes and the current approved version in use.**
- **Develop a process to monitor compliance with policies and standards.**
- **Regularly review job descriptions to make sure that the roles and responsibilities are still current and the skills and experience required are clearly specified.**
- **Perform a Business Continuation Plan risk analysis and testing annually (or when significant changes occur) and update the plan regularly to ensure its contents are complete and accurate.**
- **Prepare a quality management plan, defining the quality assurance process and how it will be implemented, for each system project as required by the adopted standards.**
- **Develop a process to monitor overall information technology performance by comparing actual performance to the capacity and technology plan on a regular basis.**

UNIX operating system

- **Set the passwords for the production servers to different passwords from those in the test and development environments.**

Oracle database

- **Identify high-risk information in the Oracle database, implement an audit log—that cannot be altered—that records changes made to this information and assign an individual to review the audit logs regularly and follow up on any unusual activity.**

Firewall access

- **Restrict access to the test and development servers to only those IP addresses that require access.**
- **Determine the appropriate IP addresses for access to CAS and restrict the firewall rules accordingly.**
- **Add a rule to the IP filter that allows only the mainframe IP addresses to use the FTP port on the database server and disables the service on the other servers.**
- **Add a rule to the IP filter that allows only the TELNET port to be used on the servers that require TELNET.**
- **Develop a process to notify support staff when the firewall is not running.**
- **Review, along with Common IT Services, the current firewall single-point of failure configuration to determine if a more secure configuration can be devised.**

Appendix B

Office of the Auditor General: 2005/2006 Reports Issued to Date

Report 1 – April 2005

Follow-up of the Recommendations of the Select Standing Committee on Public Accounts contained in its Fourth Report of the 3rd Session of the 36th Parliament: Earthquake; Performance Audit

Report 2 – May 2005

Joint Follow-up of 2001/2002: Report 1 Managing Interface Fire Risks and Firestorm 2003 Provincial Review

Report 3 – June 2005

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

This report and others are available on our website at http://www.bcauditor.com

Compiled and typeset by Graphic Designer, Debbie Lee Sawin, of the Office of the Auditor General of British Columbia
and published by the Queen's Printer for British Columbia©
Victoria 2005