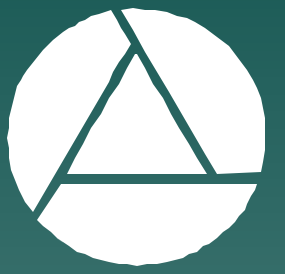
2002/2003: Report 10



OFFICE OF THE

Auditor General of British Columbia

Adopting Best Practices in Government Financial Statements – 2001/2002

National Library of Canada Cataloguing in Publication Data

British Columbia. Office of the Auditor General.

Adopting best practices in government financial statements.–2001/2002–

(Report)
Annual.
Report year ends Mar. 31.

Continues: British Columbia. Office of the Auditor General. Report on government financial accountability for the ... fiscal year. Report on the ... public accounts. ISSN 1488–4585.

ISSN 1705-1630–Adopting best practices in government financial statements

1. Finance, Public – British Columbia – Accounting – Periodicals. I. Title. II. Series: British Columbia. Office of the Auditor General. Report.

HJ13.B7B74 352.4'39'0971105 C2001–960288–X

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 604 660–2421

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://www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

The Honourable Claude Richmond
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 2002/2003: Report 10 on Adopting Best Practices in Government Financial Statements.

Wayne Strelioff, CA
Auditor General

Victoria, British Columbia
March 2003

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

Table of Contents

Project team:

Senior Principal: *Keyvan Ahmadi*

Part 1:

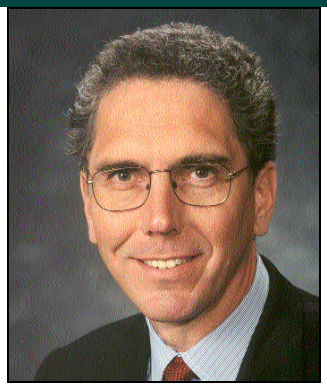
Geoff Stagg
Tony Timms
Mike McStravick
Laurie Selwood

Part 2:

Faye Fletcher
Jamie Orr
Pam Hamilton
Randy Nicholson
Kanwaljeet Kuckreja

As well, more than 40 other staff of the Office took part in the audit of the Summary Financial Statements and in the separate audits of various government organizations that are included in the government reporting entity.

Auditor General's Overview



Wayne Strelioff, CA
Auditor General

For financial accounting and reporting, the government is committed to fully adopting—by April 1, 2004—the Canadian generally accepted accounting principles for senior governments. These principles are set by the Canadian Institute of Chartered Accountants (CICA). This commitment represents significant progress, and for that I commend and strongly support the government in its decision.

Broadly speaking, Canadian generally accepted accounting principles (GAAP) cover two main areas: *accounting policies* (for example, guidance on which organizations to include in consolidated financial statements and how to account for the many and varied transactions that occur throughout the year); and *reporting standards* (which set out objectives to be followed in the preparation and presentation of the financial statements). In today's world, where public trust in corporate business and the institutions of government is low, adopting best practices in financial accounting and reporting, i.e adopting GAAP fully, is an important step forward.

My purpose in this report is to bring Members of the Legislative Assembly and the public up to date on government's progress in adopting GAAP in both accounting and reporting.

In adopting GAAP for its accounting policies, I am pleased to say that the government has made significant progress. It already follows most of the GAAP requirements, the main exception being that related to the composition of the reporting entity—an issue which it has been studying recently. The composition of the reporting entity is a matter that, in my view, is the most important one the government must finalize. I say this because I believe the Summary Financial Statements of the Province should provide a full accounting of the financial affairs and resources for which the government is responsible. At present they do not.

For the 2001/02 fiscal year, I expressed a qualified audit opinion on the Summary Financial Statements because they did not include the complete planned and actual financial results of schools, universities, colleges and hospitals. In my opinion, the government is responsible for the financial affairs and resources of these organizations, and must therefore be accountable for the overall state of their finances.

I understand that the Comptroller General and members of the government's accounting policy advisory committee share my views on this issue—for the most part. Universities, they believe, should remain excluded from the government reporting entity. It is my view, however, that the government controls the financial affairs and resources of the public universities in British Columbia, and so their financial results should be accounted for as part of the government reporting entity.

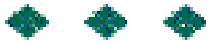
As for the reporting side of GAAP, the government has made significant progress here as well. The financial statements are now timely and provide useful information by major segment about the assets, liabilities, revenues and expenses of Crown corporations. GAAP directs that "Financial statements should communicate information that is relevant to the needs of those for whom the statements are prepared, reliable, comparable, understandable and clearly presented in a manner that maximizes its usefulness." I believe that adopting GAAP in terms of providing relevant information, and in a way that maximizes its usefulness, is as important as adopting the accounting policies required by GAAP. For this reason, I offer some suggestions and recommendations in my report as to how government can improve the quality of its financial statements, such as by improving its financial reporting by segment of responsibility.

Other recommendations I have made in my report address the accounting polices used in school districts, the consistency of distributing interest expense, and the consistency of reporting contingent liabilities. I also comment on six important transactions that took place in the 2001/02 fiscal year. This information will, I believe, help legislators and the public better understand these transactions and how they affect the overall financial results of the government.

In the second part of this report, I include our assessment of a major computer operating system, or platform, called MVS. This platform supports many of the government's important financial and operational systems. A very high level of security and control is thus expected to be at work to minimize risks to a manageable level. Our audit was designed to determine if management had set appropriate control objectives and had established procedures to meet those objectives. The control objectives were derived from guidelines set out by the CICA.

We found that all of the procedures outlined by management were suitably designed to meet the control objectives, and most procedures were in place. In some cases, however, actual practice did not follow the intended procedures. Because of these weaknesses, we concluded that not all of the control objectives had been met, meaning that the actual risk of a security breach occurring was higher than that considered acceptable. We are pleased that the Ministry of Management Services is addressing all of the weaknesses we found.

In closing, I wish to acknowledge and thank all those who assisted and cooperated with my Office during the preparation of this report, and during the course of our work on the various audits and assessments that led to the matters reported herein.



Introduction

This Report is Our Update on Government's Adoption of Best Practices in Financial Statement Reporting

Examination of the Summary Financial Statements of the Government of the Province of British Columbia is a significant focus of the work of our Office. These statements are a main component of financial accountability and transparency for the range of activities for which the government is responsible.

In examining these statements, we have two objectives. First is to provide assurance to the citizens of British Columbia that the statements present fairly the financial position and results of operations of the government. Second is to comment on the government's practices in bringing its Summary Financial Statements together and presenting them to the public.

We met our assurance objective in July 2002 when we issued our audit report on the Summary Financial Statements of the Province which was published with them. In that report we said that those statements, with some important exceptions, present the government's finances fairly in accordance with the accounting policies that are generally accepted in Canada for such statements. The matter that caused us concern was about the completeness of the Summary Financial Statements, as outlined in our report (and reproduced here in the sidebar).

This current report is intended to brief members of the Legislative Assembly and the public about the government's progress in adopting best practices in its financial accounting and reporting. Where needed, recommendations are also offered for improving those practices.

We have organized the report in two parts. Part 1 is a commentary on issues related to the statements. Part 2 is our audit report on the information technology that supports many important government financial activities.

> In note 1 to these financial statements, the Government reports that its stated accounting policies are not fully consistent with generally accepted accounting principles for senior governments as recommended by the Canadian Institute of Chartered Accountants. Consequently, these financial statements do not include the complete planned and actual financial results of school districts, universities, colleges and institutes, and health care organizations.
>
> Had a complete accounting been provided as at March 31, 2002, it would be expected that financial assets increase by $2,828 million ($2,531 million at March 31, 2001), liabilities increase by $3,102 million ($2,535 million at March 31, 2001), non-financial assets increase by $3,129 million ($2,728 million at March 31, 2001), and the accumulated deficit decrease by $2,855 million ($2,724 million at March 31, 2001). Similarly, for the year ended March 31, 2002, revenues increase by $2,214 million ($1,841 million for 2001), expenses increase by $1,989 million ($1,787 million for 2001), and the annual deficit decrease by $225 million (surplus increase by $54 million for 2001).

We Acknowledge Government's Focus on Adopting Best Practices in Its Financial Accounting and Reporting

Just as the financial statements of large corporations include the results of all their operations world-wide, so do the Summary Financial Statements, by definition, include the results of all the government's operations for its ministries, Crown corporations and other organizations.

Publishing the annual Summary Financial Statements is the result of a significant year-round effort. Many information systems process individual transactions daily and then combine them into accounts and balances that are subsequently used in creating the provincial statements. In processing transactions and accounting for them the governments are diligent in ensuring the integrity of the financial information they publish. Adopting best practices based on the Canadian generally accepted accounting principles (GAAP) helps the governments achieve this goal.

All senior governments in Canada publish Summary Financial Statements. However, not all follow the same practices in every aspect of producing them. For example, the financial reporting regime across Canada is the same, but it is not applied uniformly. While this situation does not always make it possible to compare results, it does provide us with a range of practices against which we can compare ours and determine best practices.

Selecting the best practices requires appropriate interpretation of GAAP. Therefore, it calls for the exercising of significant professional judgement. To ensure objectivity in our judgement, we consider the following in our decisions.

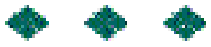
- *The generally accepted accounting principles of the Canadian Institute of Chartered Accountants (CICA).* These principles, particularly those developed by the Public Sector Accounting Board (PSAB) of the CICA, provide us with a common baseline for accounting and reporting.
- *The CICA's publications, particularly the Information Technology Control Guidelines.* These guidelines give us a benchmark for assessing control practices, especially for computer-based systems and processes.

- *The views of the members of the Canadian Council of Legislative Auditors.* These views provide us with the Canadian context.

Today, the British Columbia government is either currently following or has committed to adopt most of Canada's best practices in its financial accounting and reporting. For example:

- The Summary Financial Statements are being published earlier each year, and the government is working towards issuing them within three months of the year-end.
- The financial statements are presented on the expense basis of accounting, fully recognizing the cost of physical assets over their useful lives.
- The government is committed to fully adopting the Canadian Generally Accepted Accounting Principles in 2004/05. We expect schools, universities, colleges and hospitals soon to be consolidated in the provincial financial plans and statements.
- The corporate accounting system is being continually improved to benefit from facilities afforded by an enterprise-wide system.

We are pleased with the government's focus on improving its practices in bringing the Summary Financial Statements together. We also recognize, however, that much still needs to be done.



Part 1:
Financial Statement Issues

Part 1: Financial Statement Issues

All Issues We Come Across Are Addressed But Only a Few Result in a Reservation

An entity's financial statements are prepared by management which, in the case of the Province, is the government. The entity's auditor attaches to those statements an independent certification of the information presented in them. If, in the auditor's opinion, the financial statements do not give a fair presentation and the difference between the actual results and the reported results is significant, then the report is released with a reservation. The purpose of the reservation is to alert readers of the financial statements to the auditor's conclusions and, where possible, to provide sufficient information so readers can see for themselves what the problem is.

In any financial statement audit, it is inevitable that we take issue with the adequacy of control processes and the accuracy of financial transactions or the way they are presented. We don't expect to find every error and all control weaknesses, but we do our audit work so that we can be confident we will discover any significant ones. From those we find, we need to decide if one or more of them (individually or in aggregate) is sufficiently important that, if not corrected, it could undermine the integrity of the statements. In such a case we explain the issue in our reservation. And, to resolve the issue, we discuss the matter with officials of the government during the audit. Findings are only reported publicly if the issues are significant and not corrected, or if corrected, they could provide a lesson to improve future practice.

In British Columbia, the Government Reporting Entity Is the Most Important Financial Statement Issue

The financial reporting universe of an organization is often referred to as its reporting entity. The government reporting entity does not only define the scope of activities covered by the Summary Financial Statements, but it has also been used by governments to notify the public about what is—or is not—controlled by the government.

For financial reporting purposes, the concept of *control* presents a sound logical argument for what should be included in an entity.

It is generally accepted that a government should not be held accountable for organizations it does not control. This is PSAB's view. The government reporting entity, says PSAB, should comprise the organizations that are controlled by the government.

In British Columbia, we have always agreed with the government on what it included in its financial reporting entity, but we have not agreed with all exclusions it made. For many years we held that schools, universities, colleges, hospitals and two small Crown corporations (British Columbia Investment Management Corporation and British Columbia Pension Corporation) should be included in the government reporting entity, and that their operations should be consolidated in the Summary Financial Statements. We also discussed with government the advisability of including in the reporting entity the Workers' Compensation Board. We believe that none of the mentioned organizations has unilateral power to act independently and govern their own financial and operating strategic policies. Rather, they are substantially controlled by legislation and affected by the government's public policy decisions.

For many years, the government has disagreed with our view about these organizations and has not included them in its reporting entity.

The two small corporations are management type companies, and although their responsibilities–in terms of funds left in their care—are enormous, their own assets, liabilities, revenues and expenses are relatively small, and therefore their exclusion from consolidation does not materially affect the government's financial statements. We have not qualified our opinion on the government's financial statements on this account, and the government remains unwilling to include them.

The Workers' Compensation Board (WCB) is an organization that has recently gone through significant change in its relationship with the government and in its governance structure, to the extent that the government no longer controls its destiny. In 2002, the government agreed to produce adequate financial information on WCB in a note to its financial statement and to look after the need for public financial accountability about the organization. In turn we agreed to keep an eye on how the new arrangement will unfold.

The exclusion from the reporting entity of schools, universities, colleges and hospitals (the "SUCH" sector) results in a much larger issue.

A fundamental accounting principle that tests the integrity of a government's financial statements is that the Summary Financial Statements must provide an accounting of the full nature and extent of the financial affairs and resources for which the government is responsible—including those related to the activities of government agencies and enterprises. We have in the past maintained that because the provincial government is empowered to control the public organizations in education and health, it should provide a full accounting of the SUCH sector in its Summary Financial Statements.

In 1996, the government agreed to do this, but reversed that decision in the following year. Thus, for each year since 1997, the Summary Financial Statements of the government have both provided an explanation as to why the SUCH sector has been excluded and quantified the effect of such exclusion. Not until the Budget Transparency and Accountability Act was amended in 2001 did the government—committing itself to implementing generally accepted accounting principles for senior governments by 2004/05—consider including the SUCH sector again in its reporting entity.

We have carefully watched the government's process for determining which of the organizations in the SUCH sector should be included in the reporting entity. That process has involved a review by an advisory committee of respected non-government individuals appointed by the Minister of Finance, as well as the soliciting of advice from other sources such as the Comptroller General.

We understand that both the advisory committee and the Comptroller General agree that school districts, colleges and institutes, health authorities and hospital societies should be included in the government reporting entity. They also believe that regional hospital districts are operating outside the government reporting entity—a situation we studied as well and conditionally agreed to, provided that appropriate changes are made to legislation removing some of the government's powers over the regional hospital districts.

This leaves universities as the last issue concerning the government reporting entity at this time.

We have heard the views of the advisory committee and senior government officials as to why all public universities should be excluded from the government reporting entity (Royal Roads University is the exception because government control over that university is not disputed). These views, supported by rigorous deliberations, confirm that, of the SUCH sector organizations, the universities are the toughest cases when it comes to applying professional judgment to decide whether or not they are, for accounting purposes, controlled by the government.

For these reasons, and in anticipation of PSAB's proposed amendments of its standards on the government reporting entity, we decided to re-examine our position. After considering the weight of evidence supporting government's current controlling powers however, we again concluded that we are not able to justify excluding universities from the government reporting entity.

In our view, under its current mandate, the government is substantially responsible for the financial affairs and resources of universities because it:

- appoints and removes the majority of members of the board of governors (although two of the government's appointees are selected from among people nominated by the alumni associations),
- approves new and substantially-updated university degree programs,
- approves any operating deficits,
- approves borrowing for capital acquisition, and has access to the assets acquired by capital advances it has made,
- has the power to cause the mandate of universities to be amended,
- has the right to restrict the largest single source of revenue that universities have, and
- approves the disposal, mortgage or lease of land and the lease provisions.

The government, while respecting universities' institutional autonomy and their degree granting roles, also makes public policies that affect the direction universities must take (a policy might stipulate, for example, doubling the annual number of graduates in computer science over five years).

The public universities' financial affairs are the public's business, and their assets are substantially financed from the public purse.

The University Act stipulates that the government must not interfere in the formulation and adoption of academic policies and standards, admission and graduation, and appointment of staff. Other than these limitations (likely designed to guarantee academic freedom of universities) the government is not barred from any other involvement in the affairs of public universities. That includes involvement in their finances.

Government advisors say they have followed PSAB's current thinking on what should be included in the government reporting entity. In our view, however, what PSAB has put forward as the test of control places universities in the "controlled by government" category. According to PSAB, if government has the power to control an organization, that is sufficient reason for including it in the reporting entity. So, while we, as well as the government, acknowledge and respect universities' academic freedom, we also believe, under current legislation, that government has the power to control their financial and operating policies. Whether the government chooses to exercise that power is another matter.

When we re-examined this issue, we also reconsidered whether, in arriving at our conclusion, we might have mis-interpreted:

- the complexity of the relationship between the government and universities,
- the current thinking of PSAB on control, and
- the extent of institutional autonomy (a very old tradition cherished by universities in protecting their academic freedom against external authorities).

We wanted to be sure we had not made a judgmental error in developing our rationale for including the universities in the government reporting entity.

What we concluded was that even if the government were deemed not to control universities, it still has the ability to affect their strategic operating, investing and financing policies. The CICA Handbook refers to such ability as "significant influence" and requires that financial information of organizations so influenced be captured in the reporting entity. Factors that may indicate a situation of significant influence include representation on the board, the existence of an economic interest, and participation in the policy-making process. All factors that we think exist in the current circumstance:

- The government has a sizable representation on the board of governors of universities. The shared governance structure in place at universities requires that plans and policies formulated by the university's senate be endorsed by the board of governors.
- The government's legislated responsibility to approve the public universities' capital borrowing confirms the government's economic interest in them.
- The Ministry of Advanced Education service plan identifies as one of its five core businesses that of providing leadership and direction to universities and colleges, establishing policy and accountability for them, and providing the majority of funding to them.

Applying the "significant influence" test confirms the reasonableness of our conclusion, that excluding universities from the Summary Financial Statements cannot be justified at this time.

Aside from the question of inclusion of universities in the government reporting entity, a second fundamental question is: If the government is not accountable for the finances of the system of public universities in British Columbia, then who is? In our view putting a satisfactory consolidated accountability regime in place for universities and including the result in the Summary Financial Statements would go a long way in answering this question.

Overall, we are very pleased to see how the government has directed its efforts in resolving the reporting entity issue. We look forward to seeing the financial operations of schools, universities, colleges and hospitals being included in the Government's Summary Financial Statements.

The Reservation on Presentation of Net Liabilities Is No Longer Needed

Generally accepted accounting principles for senior governments, as recommended by the CICA, require that governments present their statement of financial position in a particular way so that their net liabilities can be clearly seen.

In 2000/01 the government did not follow the required presentation, and so we included an additional reservation in our audit report concerning that point. In 2001/02, we are pleased to report, the reservation is not needed because the government did comply with the recommended presentation.

We Discuss Other Significant Issues and Recommend Improvements

In our audit, we came across a number of significant issues we believe the government should work on with a view to adopting best accounting and reporting practices. They involve:

- using appropriate accounting policies in school districts,
- improving the way interest expense is disclosed,
- bringing consistency to the reporting of contingent liabilities,
- improving the accounting for segmented financial information, and
- resolving the problem of financial statements of school districts being for a different fiscal year than the government's.

Not included in this list are the less significant items we have reported directly to the appropriate ministries, Crown corporations and other government organizations.

Using appropriate accounting policies in school districts

The Ministry of Education has initiated a comprehensive review to improve the accounting and financial reporting of school districts. The aim is both to promote the use of appropriate accounting policies and to achieve a greater degree of consistency in the way in which the school districts report their financial performance. This review is timely because, in compliance with the Budget Transparency and Accountability Act, the government must fully adopt generally accepted accounting principles for senior governments by the 2004/05 fiscal year in its Summary Financial Statements.

The ministry has determined that the most appropriate accounting principles for school districts are those recommended by the CICA for not-for-profit organizations. Among the matters included in the ministry review are the allocation and amortization of tangible capital asset costs and the recording on a more accurate and consistent basis of the year-end liabilities for employee future benefits.

We previously reported that the ministry's deadline for completing its review was June 2002. This deadline has been extended to June 2003.

We recommend the Ministry of Education complete its review of school district accounting and reporting issues by the end of the 2002/2003 school year.

Improving the way interest expense is disclosed

The Statement of Operations in the Summary Financial Statements groups government expenses by function, such as health, education and social services, and allocates interest expense related to them. However, the part of the government's interest expense which is not allocated to other functions is separately disclosed. In our view, this accounting treatment results in misleading information.

Some years ago, the government started to allocate interest to its health, education and transportation functions, but the process stopped there and did not continue for the other functions.

To be consistent, we think the government should allocate the remaining interest, based on a reasonable rationale, over its other relevant functions.

The total interest expense is clearly shown in a note to the Summary Financial Statements.

We recommend the government be consistent in how it allocates interest expense to appropriate functions.

Bringing consistency to the reporting of contingent liabilities

The Province is a defendant in a number of legal actions and involved in matters such as expropriation compensation disputes, tax assessment appeals, aboriginal land claims and other outstanding claims. Each of these areas represents contingent losses and may involve a future expenditure of assets, including payment of cash, land or some other type of remuneration.

Depending on the circumstances, these contingent losses are accounted for in one of two ways. If the amount of future expenditure can be readily estimated and is likely to be incurred, then the estimated cost is accrued as a liability in the financial statements. The actual amount accrued is usually not disclosed, because disclosure could prejudice attempts to settle the matter out of court. If the amount cannot reasonably be estimated or if the likelihood of loss cannot be determined, then the details of the issue at hand are only disclosed in the notes to the financial statements so that a reader is aware of the matter. A portion of the amount might be accrued and an additional amount disclosed in the notes to the financial statements if the government believes it is likely a certain amount will be paid on a possible further exposure to loss.

When a contingent loss is disclosed, it is a generally accepted principle that the nature of the contingency should be adequately explained, as well as the reason why no accrual has been made (which will be that the amount cannot be estimated or the likelihood of liability cannot be determined). Often, the amount disclosed is the amount claimed in the lawsuit.

We believe that the current note covering contingent liabilities and commitments does not adequately follow this practice. It includes no explanation about a potentially large contingency, while being perhaps overly detailed for other matters. For example, the Province is a defendant in a lawsuit for alleged negligence resulting from the construction of leaky condominium buildings. The likely outcome of this lawsuit cannot be determined with certainty, but it could be substantial. Yet the contingency note does not refer to this matter specifically.

In our view, we think readers of the financial statements would be better served with pertinent information about all the significant possible contingent losses. More detailed disclosure about an issue, if desired, could be provided separately as part of management discussion and analysis about the financial statements.

We recommend the note disclosures about contingent liabilities be written in a way that reflects a level of disclosure appropriate to the relative significance of the issues.

Improving the accounting for segmented financial information

Reporting segmented financial information has been a private sector practice for some time. Doing the same in government would, we believe, help readers of the financial statements better understand the finances of the key segments of government in the context of its overall financial performance. Those key segments would include, for example, education, health, natural resources, social services, transportation, protection of persons and property, and general government. And the financial results reported for each segment would cover their revenues, expenses and, ideally, assets and liabilities.

At present, the Summary Financial Statements provide supplementary statements of "Financial Position by Sector and Results of Operations by Sector." These show some of the assets, liabilities, revenues and expenses of government's segments. However, the analysis is incomplete, since the operations of ministries have not been allocated by sector. For example, the financial results and assets and liabilities employed by the Ministries of Education and Advanced Education are not

included in the financial information of the education sector. All that is shown as segmented (or sectoral) financial information are the results of the Crown corporations and other government organizations considered to be operating in those segments. These supplementary statements are also incomplete because the government excludes school districts, universities, colleges and institutes, and health care organizations from education and health sectors in its financial reporting.

We recommend the government annually provide, in the Summary Financial Statements, complete segmented financial information.

Resolving the problem of financial statements of school districts being for a different period than the government's

The government's plans to comply fully with generally accepted accounting principles will likely result in consolidating school districts in its Summary Financial Statements for the 2004/05 fiscal year. However, the fiscal year-end of the government is March 31 and that of the school districts is June 30. Practically, therefore, the latest available audited financial statements of school districts are for the year ended nine months prior to the government's year-end. The government must ensure the operating results of the school districts between July 1 of one year and March 31 of the next year are reported as completely and accurately as possible in its Summary Financial Statements.

We noted earlier in this report that school districts along with universities, colleges and institutes, and health care organizations (the SUCH sector) are not currently consolidated in the Summary Financial Statements. The impact of the activities of these organizations on the financial statements is shown, however, in an unaudited schedule in the Public Accounts. The schedule includes an estimate, rather than audited information, of the operations of the school districts for the year ended March 31. The coming consolidation will therefore require the use of assumptions regarding, for example, the determination of school districts' tangible capital asset costs, amortization, and the allocation of operating costs over the April 1 to March 31 period. While these assumptions may be appropriate for unaudited supplementary

information, some uncertainties associated with them would limit their use for preparing an audited financial statement.

One solution is for school districts to produce audited financial statements for their third quarter. When the results of school districts were included in the Summary Financial Statements for the first time, in 1995/1996, the government produced such audited information based on the school districts' financial year-end of June 30, 1995. That required considerable additional work to ensure the information accurately reflected not only the operations for the period from April 1, 1995 to March 31, 1996, but also the assets and liabilities as at March 31, 1996. In that year, the Summary Financial Statements were not finalized until November 1996.

Changing the statutory year-end of school districts to March 31 may be another solution for preparing the Summary Financial Statements, but it is not a logical year-end choice for school districts.

A workable option might be for school districts to prepare an interim financial statement, as at March 31 of each year, for inclusion in the Summary Financial Statements. Nevertheless, if it took this approach, the government would still need to seek an appropriate level of assurance regarding the reasonableness of the interim financial information.

We recommend the government consider the possibility of obtaining assurance on an interim financial statement of school districts as at March 31 each year, for inclusion in the Summary Financial Statements.

We Discuss the Financial Effects of Important Decisions on the Summary Financial Statements

The Summary Financial Statements are complex and serve a general purpose. In putting them together annually, the government summarizes a great deal of information, including that about significant transactions which are either non-recurring or have occurred for the first time. A fuller explanation helps readers understand the role these transactions play in shaping the government's finances. We discuss six such transactions that

played a significant role in shaping the financial statements of the government in 2001/02:

- recording equalization payments,
- accounting for the federal government's overpayment of mutual fund tax revenues,
- accounting for the government's restructuring exit expenses,
- reporting the gain on pension settlement,
- calculating the Province's cost to support Skeena Cellulose, and
- disclosing the government's equity in BC Hydro.

Recording equalization payments

Equalization is a program of the federal government that is intended to reduce fiscal disparities among provinces. Payments under equalization are intended to enable less prosperous provincial governments to provide their residents with public services that are reasonably comparable to those in other provinces.

The calculation of equalization payments is a complex process. The first step is to calculate the per capita revenue of the Province. This involves determining more than 30 types of revenue following procedures and formulae set out in federal legislation and using average tax rates. The same calculation, using the same formulae and rates, is done for each province so that the results will be directly comparable.

Next, the national standard is determined by averaging the per capita incomes of the five "middle income" provinces: British Columbia, Saskatchewan, Manitoba, Ontario and Quebec.

Any province whose per capita income is less than the standard is entitled to receive payments to bring its per capita revenue up to the national standard.

In 2001/02, British Columbia received $226 million in equalization payments. Of this amount, $94 million was for 1999/2000 and the remainder was for 2001/02. No payments were due to the Province for 2000/01 because of strong energy revenues earned from natural gas royalties and electricity sales.

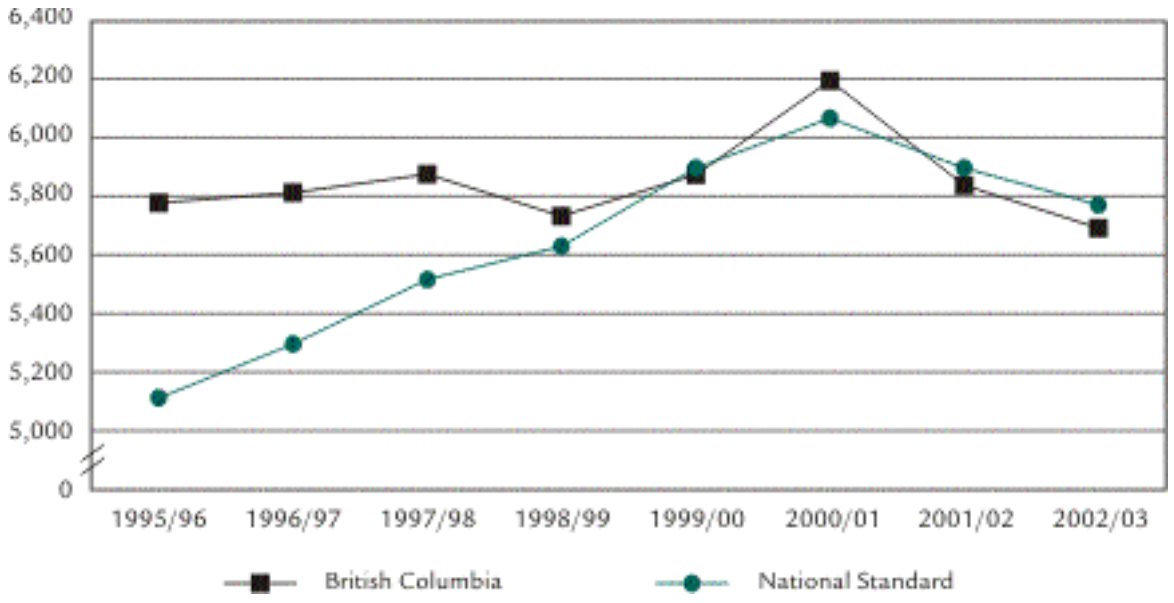
Exhibit 1.1 shows the per capita income in British Columbia and the national standard since 1995/96, with a projection forward to 2003.

More recently, in the Estimates for the fiscal year ending March 31, 2004, the government has estimated that British Columbia will receive $668 million in 2002/03. Receipts under the federal equalization program are recorded on a cash basis (as opposed to an accrual basis). In other words, the Province records the payments as and when they are received, and does not try to account in the financial statements for what might be received in later years for a current year.

We agree with the government recording the equalization payments on a cash basis. Estimating what a province may receive is complex, subject to significant uncertainty, and potentially unreliable for financial statement purposes. For example, federal estimates in October 2001, halfway through the year, showed no

Exhibit 1.1

Per Capita Income for British Columbia and the National Standard, 1995/96 – 2002/03



Source: Department of Finance, Ottawa, February 27, 2002, official estimates

equalization payments would be made to British Columbia. Those estimates were later revised and in the end the Province received $226 million in March 2002.

Accounting for the federal government's overpayment of mutual fund tax revenues

Mutual fund trusts pay federal and provincial income taxes on the taxable capital gains made in the funds. However, the trusts also report those gains on T3 slips, which they issue to individual unit holders to include on their own returns. The trusts can then claim a refund for the amount of taxes due on the gains shown on the T3s. In the end, the mutual fund trusts pay little or no tax on these gains, with the tax being paid instead by the individual investors.

The federal government requires mutual fund trusts to show separately on their tax returns the amount of tax owing and the amount of the refund claimed. The taxes and the refunds are segregated into the appropriate federal and provincial amounts.

The federal government records the amount of provincial taxes owing by the mutual fund trusts, along with all the other provincial taxes it collects on behalf of the provinces, so that it can pay the provinces the taxes it has collected for them. However, because of an accounting error, for many years in the past the federal government did not deduct the refunds of provincial taxes claimed and collected by the mutual fund trusts. As a result, it transferred more money to the provinces than it ought to have.

This error has likely existed since the 1970s, although the refunds have only become significant in the last 10 years with the dramatic growth in mutual funds and the period of notable gains in the stock market. Recently, the error was noted and investigated by federal government internal auditors and reported to the Auditor General of Canada, who confirmed their findings. To provide additional assurance to the provinces, the Canadian Council of Legislative Auditors formed a working group to review the work of the Auditor General of Canada. Our Office was part of that group.

The amount of the error that affects British Columbia is $121 million for 1999 and earlier tax years, $58 million for the 2000 tax year, and an estimated $35 million for the 2001 tax year. The Province is of the opinion that the liability for the errors

relating to the 1999 and earlier tax years is the responsibility of the federal government. Accordingly, it has not made any accrual for repayment. Instead, the amount is disclosed only as a contingent liability. (In September 2002, the federal government stated it would not request repayment from British Columbia for those tax years.) However, as the federal government's books on the tax years 2000 and 2001 are still open, the amounts related to those two tax years will be deducted by the federal government from the transfer of taxes to the Province. The adjustment for the two years are correctly made in the Summary Financial Statements of the prior and current years.

The tax year is the calendar year, which is different from the fiscal year of the government (ending March 31). The adjustment to the Summary Financial Statements, taking into account the different year-ends is as follows:

Impact on fiscal year (in $ millions)

	Error	1999-2000	2000-2001	2000-2002
2000 tax year	58	15	43	
2001 tax year	35		9	26
total		15	52	26

Accounting for the government's restructuring expenses

The British Columbia government has embarked on a significant restructuring of government operations. This is resulting directly in expenditures that are not associated with the continuing activities of government such as penalties paid to cancel contracts not needed as a result of the restructuring.

The restructuring is to be carried out over three years. As each relevant restructuring plan is approved, associated costs are recorded. Thus, in the 2001/02 Summary Financial Statements, the costs recorded are those for which restructuring plans had been approved prior to March 31, 2002. Further costs will be incurred in the future.

In accordance with generally accepted accounting principles, the cost to the Province of restructuring government ministries

and fully consolidated Crown corporations and agencies is shown separately in the Summary Financial Statements, as an unusual item on the Statement of Operations. In 2002, the restructuring cost was a total of $224 million: $161 million for government ministries, and $63 million for the fully consolidated Crown corporations and agencies.

Both the Insurance Corporation of British Columbia (ICBC) and BC Rail also incurred restructuring costs. However, because they are government business enterprises, these costs are not fully consolidated in the Summary Financial Statements. The Province accounts for these organizations using a modified equity basis. This means that only their net earnings from operations are included in these statements and their restructuring costs, although deducted in arriving at their net earnings, are not shown separately. In 2001/02, the restructuring costs totalled $40 million for ICBC and $165 million for BC Rail. The cost for all government organizations in 2001/02 was therefore $429 million of which $114 million was due to severance.

Reporting the gain on pension settlement

For many it is difficult to understand how, in the 2001/02 fiscal year, the government earned an income from public sector pension plans. An accounting explanation is provided in a note to the Summary Financial Statements, but it is complex. Does the significant earning that reduced the annual deficit by approximately $1.5 billion represent real money?

A pension plan is like a savings account. Every month, premiums collected from members and their employers are paid into the plan, and retirement pension amounts are paid out of it. Also paid into the plan is the interest earned from investing plan assets. At any given time, the plan assets may or may not be sufficient to meet the plan's obligations to retired members and the future retirees. Any excess value of plan assets over its liabilities places the plan in a surplus position. Deficit arises when the plan's obligations are estimated by actuaries to be greater than the value of assets.

Actuarial valuation—a very complicated and lengthy estimation of the financial health of a plan—is normally done every three years using models and equations developed over

time. These estimations are the best financial information available to employers and members, and are reasonably accurate. Sometimes, however, the financial market will not behave as expected by actuaries. A new actuarial valuation may therefore result in an improved or deteriorated estimate of the plan's financial position. In a very stable financial market these fluctuations might be small. In a changing market—such as what we have experienced in the last decade—the fluctuations can be substantial. Given the very large sums that pension plans invest, the change may result in substantial valuation gains or losses.

Because of the long-term nature of a pension plan, it is not considered prudent to recognize the experience gains or losses immediately every time the actuaries predict a large improvement or a sizable drop in the value of plan assets. The CICA recommends that changes between the two actuarial periods be amortized over a number or years to smooth the effect of the change on the operation of the entity. The period over which the experience gains or losses are amortized is the estimated number of years an average retiree expects to benefit from the plan. Currently this period is around 12 years.

In 1999, the Public Sector Pension Plans Act set in motion joint trusteeship agreements concerning the management of the four public sector pension plans: the College Plan, the Municipal Plan, the Public Service Plan, and the Teachers' Plan. Joint trusteeship agreements were signed for the College and the Public Service plans during 2000/01, and for the Municipal and Teachers' plans were signed during 2001/02. Though in the eyes of members the plans continued without a visible break in them, in real terms, the joint trusteeship agreements ended the old plans and started the new ones. As old plans ended, so did the government's unilateral responsibility for the financial well-being of them. The new plans will be managed jointly by trustees representing employers and employees who will be sharing the responsibilities equally.

Based on information provided by the last four consecutive actuarial valuation reports the plans' finances have been improving in prior years and were all in relatively good financial position when they changed hands. However, because of the accounting practices explained above, the government has not been able to fully account for all the experience gains. Recognizing them at

once on settlement effectively wiped out the remaining balance of the government's liability for these plans, and resulted in a one-time income in 2001/02 of $1,464 million.

The joint trustees are expected to keep an eye on the financial position of the new plans to ensure they do not carry in future substantial unfunded liabilities.

Calculating the Province's cost to support Skeena Cellulose

In September 1997, the provincial government signed an agreement that formed the basis of a plan to keep Skeena Cellulose operating. There has been disclosure in the government's annual financial statements since then. In 2001/02, the provincial government sold its investment in the company.

However, the financial statements do not give an overall view of how the provincial government became involved, what it did, and how much was paid during that time.

Background

In the late 1990s, Skeena Cellulose Inc., a private forest products company located in northern British Columbia, ran into financial difficulty and was in danger of shutting down. The provincial government became involved with it in 1997 to help the company avoid closing.

On March 3, 1997, Skeena filed for protection from creditors under the Companies Creditors Arrangement Act. Its two major creditors were the Royal Bank and the Toronto Dominion (TD) Bank, each of which held 50% of Skeena's total $415 million in loans (including term debt of $330 million and an operating loan of $85 million). Ownership of the company shares was transferred to both creditors.

On September 26 that year, after several months of negotiations, a Memorandum of Lenders' Agreement was reached between the provincial government and the two banks. Forming the basis for a plan to restructure Skeena's ownership and debt, the agreement involved participation by the Pulp, Paper and Woodworkers of Canada and included the Provincial Government Job Protection Commissioner economic plan.

When the Royal Bank chose to withdraw from the restructuring plan in November 1997, the provincial government purchased the bank's ownership interest in Skeena and the term and operating loans owed by Skeena to the bank. It also assumed the Royal Bank's obligations under the Memorandum of Lenders' Agreement. The government then formed 552513 British Columbia Ltd. (552513), a Crown corporation with the mandate of holding the government's share ownership of Skeena and providing the funding agreed to under the capital expenditure loan. The new Crown corporation bought the Royal Bank's shares in Skeena, as well as the $37.5 million term loan and $42.5 million operating loan, for $31.3 million. The funds for this purchase were provided to the corporation by a loan from the TD Bank to 552513, which was guaranteed by the government through the new corporation. Eventually, 552513 became the majority shareholder of Skeena, with a 65.6% interest, and the TD Bank became a minority shareholder with a 34.4% interest. By 2001, the government, through the corporation, owned 72.3% of Skeena.

The restructuring plan made provision for Skeena's pulp mill workers to become 20% shareholders of the company based on the workers' agreed-upon wage cut of 10% over seven years. Although legally entitled to the shares, the workers were never issued them because the agreement establishing the mechanism for distributing the shares among the three labour groups involved was not finalized before Skeena was sold in 2002 (discussed below).

Contributions, loans and loan guarantees made by the provincial government

Based on the Memorandum of Lenders' Agreement and subsequent purchase by the provincial government of the Royal Bank's position in Skeena, Treasury Board approved certain loans, loan guarantees and other contributions as part of the restructuring plan. Creditors approved this plan in January 1998 and Skeena formally emerged from protection under the Companies Creditors Arrangement Act in February 1998.

The originally approved funding is described briefly below (and summarized in Exhibit 1.2), along with the additional government assistance approved after February 1998:

Loan for payment to unsecured creditors

The provincial government guaranteed a TD Bank loan to Skeena for $14.5 million to pay the unsecured creditors as part of the settlement arrangements accepted by creditors in the restructuring plan under the Act.

Operating loan guarantees

Initially, the provincial government guaranteed $22 million of Skeena's operating loan of $120 million. During 1998 and 1999, three increases were further guaranteed: $15 million in June 1998; $15 million in October 1998; and up to $50 million in May 1999. This resulted in the government providing a total of $98.7 million in operating loan guarantees.

Capital expenditure program loan

The provincial government agreed to a capital expenditure program loan to Skeena of $122 million (resulting in a total possible loan of $170 million when combined with the TD Bank's loan). This loan, for making improvements to the pulp mill, was to be funded over three years. In June 1998, as a result of poor markets, the program was reduced from $170 million to $110 million, reducing the Province's funding obligation to $77.4 million. In May of 1999, the Province agreed to fund any undisbursed portion of the capital expenditure program loan at that time, increasing the Province's funding obligation to a total of $96.8 million. Of that, $92.3 million was actually loaned out.

In November 1998, the TD Bank declined making further capital expenditure program loan advances. In response, the government guaranteed a TD Bank loan to Skeena of up to $11.5 million for mandatory safety and environmental expenditures under the capital expenditure program. (At that time all program spending had been deferred except for required safety and environmental expenditures.)

Road-building loan guarantee

In July 1998, the provincial government guaranteed an $18 million loan from the TD Bank to Skeena to cover required road-building expenditures.

Wage contributions

Wage contributions of $26.9 million were approved by the provincial government to Skeena over seven years. These contributions were intended to subsidize the wage cut requested by the banks as part of the restructuring plan, effectively reducing the cut taken by workers from 17.5 to 10%. Payments under the agreement were subject to certain clauses concerning provisions of future collective agreements at other pulp mills in British Columbia. As a result of collective agreements reached by other pulp mill operations in British Columbia in 1998, the wage contributions were discontinued in 1999, after only $1.7 million had been paid.

Exhibit 1.2

Loans, loan guarantees and other contributions made by the provincial government to Skeena

($ millions)

		Fiscal year					
		1998	1999	2000	2001	2002	Total
Loans/Guarantees							
Royal Bank share purchase	Guarantee	31.3	(3.1)[1]	(3.2)[1]			25.0
Loan for payment to unsecured creditors	Guarantee	14.5					14.5
Operating loan	Guarantee	22.0	28.1	34.1		14.5	98.7
Capital expenditure program	Loan	3.0	1.0	30.2	57.3	0.8	92.3
	Guarantee		10.5				10.5
Road-building loan	Guarantee		18.0				18.0
Total Loans and Guarantees							**259.0**
Non-Repayable Contributions							
Wage offset	Contribution	.7	1.0				1.7
Road-building loan	Contribution		1.7	1.7	1.7		5.1
Total Contributions							**6.8**

[1]These reductions of the guarantee for the Royal Bank share purchase loan are a result of Skeena's interest payments being applied against the loan principal.

Source: Compiled by Office of the Auditor General of British Columbia

Road-building contribution

Under the Job Protection Commission plan, the then Ministry of Employment and Investment (now Ministry of Competition, Science and Enterprise) provided Skeena with road-building funding of $1.7 million a year for three years in order to improve the company's access to timber resources.

The Sale of Skeena

During 2001, Skeena experienced further significant operating problems, which resulted in it again seeking protection under the Companies Creditors Arrangement Act on September 5, 2001. On February 20, 2002, NWBC Timber & Pulp Ltd. (NWBC) agreed to purchase Skeena and its subsidiaries (excluding Buffalo Head Forest Products Ltd.). The new owner agreed to pay $8 million in total, $6 million to be applied against secured creditor claims (TD Bank and the provincial government) and $2 million to be applied on claims of unsecured creditors. The sale closed on April 26, 2002, and on May 8 the government, through 552513 British Columbia Ltd., received proceeds of $2.5 million for the sale of Skeena (Exhibit 1.3).

Exhibit 1.3

Amount paid to 552513 British Columbia Ltd. following the sale of Skeena Cellulose Inc. to NWBC Timber & Pulp Ltd.

Payment	$6,000,000
Fees and disbursements	202,400
Net	5,797,600
Provincial government share (52.6%)[a]	3,049,538
Less: Levy	(24,483)
Less: Trust claims filed	(557,241)
	$2,467,814

[a]This portion of the $5.8 million for secured creditors was assigned to 552513 British Columbia Ltd. as part of the restructuring plan approved under the Companies Creditors Arrangement Act on April 4, 2002.

Source: Compiled by Office of the Auditor General of British Columbia

The amount paid to the secured creditors was reduced by bankruptcy trustee fees and associated legal fees and disbursements. This resulted in a net amount of $5.8 million being paid to the government (through 552513) and the TD Bank. The net amount received by 552513 was further reduced by a levy of $24,483 (as required under the Bankruptcy and Insolvency Act) and trust claims of $557,241. The latter reduction was for stumpage that Skeena collected from logging contractors but never remitted to the government. In keeping with the restructuring plan, the third-party stumpage obligations owed by these logging contractors were paid out from the government's share of the sale proceeds.

As a result of the TD Bank calling in the loans owed by Skeena, the various loan guarantees provided by the provincial government to the bank were paid out between September and November 2001. This included $25.1 million paid on behalf of 552513 for the loan guarantee used to purchase the Royal Bank interests; $124.1 million for all term loans and the non-revolving portion of the operating loan; and $18.4 million for the revolving portion of the operating loan. The loans previously owed by Skeena to the TD Bank and paid out under the guarantees were assigned to the government. Two new companies were set up with the sole purpose of holding the assigned loans: $124.1 million went to 632121 British Columbia Ltd. (632121), and $18.4 million went to 634349 British Columbia Ltd. (634349). Both companies became secured creditors, capable of voting secured creditor claims under the Companies Creditors Arrangement Act. The loans were subsequently written off by the two companies, both of which are now being wound up.

In addition to the guarantee payouts, the government wrote off the $92.3 million loan due from Skeena (through 552513) under the capital expenditure program.

As part of the sale, the government agreed to provide Skeena and NWBC with a limited environmental indemnity of up to $30 million. Both companies are exempted from all losses, costs and expenses related to hazardous substances, and from all third-party claims for damages related to hazardous substances, incurred before the closing date of the sale of Skeena to NWBC. This indemnity terminates on the sixth anniversary of the purchase of Skeena.

The restructuring plan resulted in zero recovery on all Crown claims against Skeena:

- Skeena and its subsidiaries owed approximately $21.5 million in stumpage to the Ministry of Provincial Revenue.
- Licence and permit fees and miscellaneous taxes totalling approximately $4.2 million were written off.

Other government programs related to Skeena

Skeena's financial difficulties prompted Forest Renewal BC to establish the Credit Enhancement Emergency Fund (CEEF) loan guarantee program in 1997. This fund, administered by Collection and Loan Management Branch of the Ministry of Provincial Revenue, provided a 100% loan guarantee to financial institutions that gave loans to British Columbia companies in distress as a result of Skeena's plight. The program approved 201 loans, which amounted to $36 million in guarantees.

At March 31, 2002, there were 122 loans outstanding, worth a total of $9.9 million. The provincial government has paid out $3.27 million in guarantees for defaulted loans. And it could ultimately be responsible for the remaining $9.9 million in outstanding guarantees should all the loans be defaulted on.

The total cost of Skeena to the provincial government is over $323 million

We determined that the total amount of all direct costs incurred by the government as result of its involvement with Skeena Cellulose from 1998 to 2002 has been $323.3 million (Exhibit 1.4). That does not include the $9.9 million for loan guarantees still outstanding under the CEEF loan guarantee program described above, some or all of which the provincial government may have to pay if the debtors default. We also did not include in our calculations of this total expenditure either the lost opportunity cost of the government funds used to pay for all the expenses related to Skeena, or the economic benefits derived from keeping the mill open.

Readers should note as well that we have included only the direct costs incurred by government in supporting the company that we are aware of, after reviewing relevant documentation and having detailed discussions with the Ministry of Competition, Science and Enterprise staff.

Exhibit 1.4

Loans, loan guarantees and other contributions made by the provincial government to Skeena

($ millions)

			Loan/guarantee pay-out mechanism				
		Total	Paid by Province	Debt transfer to 632121[2]	Debt transfer to 634349[2]	Loan forgiven	**Total Cost to Province**
Loans/Guarantees							
Royal Bank share purchase	Guarantee	25.0	25.1[1]				25.1
Loan for payment to unsecured creditors	Guarantee	14.5		14.6[1]			14.6
Capital expenditure program	Loan	92.3				92.3	92.3
	Guarantee	10.5		10.7[1]			10.7
Operating loan	Guarantee	98.7		80.8	18.4		99.2[1]
Road-building loan	Guarantee	18.0		18.1[1]			18.1
Total			25.1	124.2	18.4	92.3	**260.0**
Non-repayable contributions							
Wage Offset	Contribution						1.7
Road Building Loan	Contribution						5.1
Total contributions							**6.8**
Environmental liability assumed by Provincial Government							**30.0**
Stumpage revenue write off							**21.5**
Miscellaneous fees, licences, taxes written off							**4.2**
Credit Enhancement Emergency Fund defaulted loan payments							**3.3**
Less: Proceeds from sale of Skeena							**(2.5)**
Total							**$323.3**
Contingencies							
CEEF loan guarantees							9.9
Total potential cost							**$333.2**

[1]Differences between the amount guaranteed or loaned and the amount paid or forgiven are the result of interest accruing on the amount guaranteed or loaned.

[2]After the debt was transferred to the two companies, it was written off.

Source: Compiled by Office of the Auditor General of British Columbia

Disclosing the government's equity in BC Hydro

In a rate-regulated utility company, the Rate Stabilization Account (RSA) refers to a reserve account established primarily to protect consumers against volatile energy markets. Usually, in good years—when there are surpluses—funds are transferred to this account to help pay the excessive costs that would otherwise result in higher rates in bad years. In a similar way to other utility companies across Canada, BC Hydro follows the accounting standards of rate-regulated organizations. These standards allow payments to the RSA to be treated as if they were a company expense. Similarly, any withdrawal on that account is recognized as company income. This accounting practice is peculiar to rate-regulated organizations. In other corporations (e.g. insurance companies) transfers to the rate stabilization reserve would, ordinarily, not affect the corporations' earnings.

In the 2001/02 fiscal year, BC Hydro transferred $145 million from its RSA to its operation, reducing that account's balance from $232 million to $87 million. This transfer, which was treated as income of the 2001/02 fiscal year increased the corporation's consolidated net income from $258 million to $403 million. Out of this adjusted annual net income, BC Hydro paid $333 million to the provincial government as a dividend. In effect, therefore, part of the dividend to the Province came from the RSA, which implies that the RSA is part of the retained earnings of BC Hydro and therefore should be included in the Province's equity in that company.

In the Summary Financial Statements, the government includes the balance of the RSA as part of the Province's equity. However, the balance sheet of BC Hydro does not. This raises the question: "Which set of financial statements shows the Province's equity in BC Hydro correctly?" In our view the Summary Financial Statements do. We also believe that it would be clearer if BC Hydro, instead of showing the RSA as a liability, showed its RSA as part of the government's equity.

Considering RSA as a liability—the way rate-regulated accounting standards allow—is more appropriate for a private sector utility company whose rates are determined by an independent regulator. In such a situation, the regulator can force the utility company to hold funds in a liability account

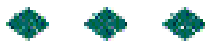
that shareholders cannot access. On the other hand, where the regulator is the shareholder, an official or agent of the shareholder (as is the case with BC Hydro), it is impossible to achieve such separation effectively.

All legislative auditors across Canada are in full agreement that, in circumstances where regulators are not independent of the rate-regulated organization, it serves little purpose for the publicly owned organization to follow the rate-regulated accounting standards.

The Canadian Council of Legislative Auditors has formally requested PSAB to revise the rate-regulated accounting standards for publicly owned corporations. In the meantime, because the current accounting standard is in place, auditors may choose not to make a reservation when publicly-owned rate-regulated utility companies follow it.

While the application of accounting standards of rate-regulated organizations does not extend to the Summary Financial Statements, in many other jurisdictions the results of this accounting standard are carried forward to the summary financial statements with no adjustment.

In preparing its financial statements, the British Columbia government has been adding back the RSA balance to the government equity for many years. We are pleased to note that this practice continued in the 2001/02 fiscal year. The result is a more accurate disclosure of the substance of RSA in the government's financial statements.



Response from the Ministry of Finance

We appreciate the opportunity to respond to the Auditor General's report. While we always carefully consider the Auditor General's comments and recommendations, we do have a number of difficulties and differences of view with this report.

As our standard, we follow the recommendations of the Public Sector Accounting Board (PSAB) of the Canadian Institute of Chartered Accountants. This constitutes a clear reference point upon which to base our accounting and is consistent with that being used by other senior governments in Canada. As the Auditor General notes, we have now adopted the "net liabilities" format for our Statement of Financial Position. We are also reviewing a number of other practices and policies of government to confirm they meet PSAB recommendations in order that we may ensure we are fully compliant with GAAP by the legislated deadline of fiscal year 2004/05. The Auditor General and the government are generally able to agree on what PSAB requirements represent. However, in a couple of areas noted in this report, we feel that the Auditor General is departing from the PSAB standard as it is interpreted in Canada.

Government reporting entity

In determining what organizations should comprise the government reporting entity under GAAP, we are using the new criteria developed by a task force of PSAB. These new criteria have been developed to deal with the concerns of senior governments that the current criteria are difficult to interpret and apply. The new criteria clearly spell out that the basis for including an organization is that the government controls it—control being defined as "… the power to govern the financial and operating policies of another organization with expected benefits or the risk of loss to the government from the other organization's activities." The criteria are very explicit in stating that this control must arise from existing legislation and provide a series of indicators of control as a test to use in applying professional judgement to the existing relationship.

The criteria are also very clear that constitutional responsibility for a particular program is not an indication of control. For instance, where an organization (e.g., private schools) delivers services which are the responsibility of government, the organization cannot be presumed to be controlled by government, nor does the fact that

government legislation creates an organization necessarily mean that government controls it. The test must be the ability to control the financial and operating policies of that organization on an on-going basis.

As noted by the Auditor General in his report, we have reviewed our current reporting entity against these new criteria. We have found that, while they do not change the status of the majority of the organizations included in the current government reporting entity, they do clarify the position of a number of entities considered questionable in the past. We have reviewed our findings with the Auditor General and found that in the majority of cases our evaluations come to the same conclusions. However, there are a number of entities where the Auditor General disagrees with our conclusion. In each of these cases, we believe he is applying a standard that is not PSAB compliant. The main group of entities in dispute is universities operating under the Universities Act and we will focus our response on those entities although, as he notes, there are other organizations in question where we have the same type of issues to resolve.

The Auditor General argues that the government has the power to control the financial and operating policies of universities. We are unable to support his conclusion on this issue. In our view, universities (except for Royal Roads University, which operates under different legislation) do not meet the new control criteria. The Universities Act does not provide the government with an over-riding control of their activities. We appoint six of fifteen board members directly plus select two more from a list provided by the university alumni. The government must also approve any operating deficits incurred by the universities, their borrowing and their disposal of land. This combination of powers does not, however, in our judgement, result in government controlling the entire financial and operating policies of universities. The controls provided are only those required for the prudent application and monitoring of the government's funding of the organization.

The other items listed by the Auditor General as indications of control arise entirely from our funding of university operations. PSAB is very clear that financial dependence on the government does not constitute control. Universities have the power to develop and establish new programs, to develop academic interests and channel their operational resources to support those activities. Any power the

government has to approve new and substantially updated programs, to cause the mandate of universities to be amended and restrict the largest source of revenue would arise from the fact that the government provides the largest single source of revenues to the universities through its grants to university operations. If the universities were to obtain funding from other sources, these powers would disappear. If we were to use this as a basis for control, we would be bringing in any organization with significant financial dependence on the government, hence PSAB's exclusion of such powers from the criteria.

The argument that someone needs to be accountable for universities clearly takes us into the realm of including organizations where we have constitutional responsibility or have legislated an organization into existence. This is not part of the criteria established by PSAB and was specifically exempted because constitutional responsibility is far too broad as an inclusion determinant. Universities are controlled by their individual boards and the boards are accountable for their operations, not the government.

As noted by the Auditor General, the government has referred this issue to the Accounting Policy Advisory Committee (APAC) for review and comments. That Committee is comprised of qualified accountants who have volunteered to provide the government with advice on issues arising from the government's commitment to move to full GAAP. The Minister of Finance received nominations for members of the Committee from the Institute of Chartered Accountants of British Columbia, Certified General Accountants Association of British Columbia, Certified Management Accountants Society of British Columbia and Financial Executive International. This group is well qualified and provides an independent viewpoint from which to consider these accounting issues.

The APAC met a number of times to consider issues referred for its consideration, including the question of whether or not school districts, universities, colleges and institutes and health care organizations (the SUCH sector) should be included in the government reporting entity. The APAC agrees with the Auditor General that school districts, colleges and institutes, and health care organizations should be included in the government reporting entity. However, APAC does not agree that universities under the Universities Act should be included.

Response from the Ministry of Finance

The APAC reviewed the legislation and discussed the relationship of universities to the government with individuals from Treasury Board Staff, the Office of the Comptroller General, the Ministry of Advanced Education and The University Presidents' Council. The unanimous conclusion of the APAC was that universities (except for Royal Roads University) should be excluded. This conclusion was in the APAC's first report to the Minister of Finance. Subsequently, because the Auditor General did not agree with this conclusion, the APAC reviewed the facts that lead to their conclusion. They again interviewed key individuals and reviewed the information. They also discussed the Auditor General's opinion directly with him. The APAC's conclusion did not change as a result of this review and it continues to recommend exclusion of universities from the government reporting entity.

We would also note that the position of the government and the APAC with respect to excluding universities from the government reporting entity is supported by the findings of most other provinces which have used these new criteria to evaluate their own reporting entity. Only the Province of Manitoba includes universities in its entity because the province controls the boards of these organizations and has access to their assets. It is expected that as provinces move forward in addressing the reporting entity issue, most will be excluding universities from their financial statements.

The Auditor General has raised the question of significant influence over universities. Significant influence as a criterion is normally applied to private sector organizations. The application of the private sector handbook provisions are questionable given the new PSAB entity criteria and in view of the differences between private sector not for profit and public sector powers and responsibilities. PSAB is considering a project to evaluate the application of significant influence criteria to government entities; however, it has not been approved at this time.

Having universities outside the reporting entity is consistent with the substance of their relationship with government. While the province is responsible for the legislative framework, and for the funding it provides, universities have significant discretion and academic freedom to manage their affairs. This is reinforced by the recent repeal of legislation that controlled universities' ability to raise tuition fees.

The universities themselves do not believe they are part of the government reporting entity as defined by PSAB. They believe that if they are included in the government reporting entity and included, for example, under the Balanced Budget and Ministerial Accountability Act, the government may be tempted to interfere with or micro-manage university affairs, perhaps leading to new legislative changes to provide overall control. Their greatest concern is that inclusion in the government reporting entity is more than an accounting issue when all the potential impacts on universities are considered. For instance, it could impact their fund raising from other sources due to a perception that the monies would be going to government rather than the university.

It is government's belief that universities meet the test for exclusion based on the most recent PSAB criteria. In the past, the Office of the Auditor General has agreed that universities were the weakest case for inclusion in the government reporting entity. The current Auditor General has stated that he could see an argument being made for exclusion, however, his preference is that government needs to be seen as accountable for the entire university system and, therefore, universities should be included.

While we do not agree with the Auditor General on the inclusion of universities in the reporting entity, we will have to include them unless the Auditor General changes his position. We view this issue, however, as a work in progress and will be monitoring the application of the new reporting entity criteria in other provinces. Further review may be required if it is found that British Columbia is out of step with the other provinces.

Using appropriate accounting policies for school districts

The Ministry of Education is in the process of completing its review on the appropriate accounting policies for school districts. However, there are administrative constraints associated with the implementation of these policies by the school districts. School districts have raised significant concerns that must be resolved prior to implementation. It is currently planned that school districts will work over the next year to implement GAAP and will begin producing GAAP based reports effective fiscal 2004/05. In the meantime, we will be testing the proposed new reporting standards and process by collecting accrual based 2003/04 data for school districts over the next year.

Improving the way interest expense is disclosed

The allocation of interest expense beyond our current practice of allocating costs associated with the capital funds provided to school districts, educational institutions, and transportation has proven more difficult than originally anticipated. We have not been able to formulate an effective allocation of the remaining interest costs to government programs that produces a reasonable result. However, we appreciate the Auditor General's concern and are, therefore, considering other options such as moving the currently allocated interest costs back to a single interest expense function. This is consistent with the reporting of other provinces and also with Statistics Canada government expense groupings. We will be further discussing this issue and options available with the Auditor General over the next few months.

Bringing consistency to the reporting of contingent liabilities

The Auditor General is recommending that we change our note disclosure for contingent liabilities to reflect the level of disclosure appropriate to the relative significance of the issue. While we agree with the recommendation and feel that our note disclosure could be improved, we disagree that additional disclosure would necessarily be the appropriate approach.

Lawsuits are very much a case in point. Often the total claim made to the courts may not necessarily be an accurate reflection of our actual potential liability. Further, providing too much detail on individual lawsuits is always a concern as it could potentially imperil our ability to achieve a satisfactory resolution.

A recent review of the contingent liability notes of other provinces has shown that our note is far more extensive than the normal practice.

Improving the accounting for segmented financial information

We are currently working on a project to improve segmented financial data contained in the audited Summary Financial Statements. We hope to have succeeded in allocating Consolidated Revenue Fund amounts to appropriate categories for the 2002/03 Public Accounts, thus resolving the major concerns of the Auditor General on that matter.

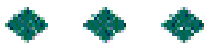
Resolving the problem of June year-end for school district financial statements

The problem of the June year-end for school districts is being dealt with as part of our project to move to full GAAP by fiscal 2004/05. School districts have indicated their concern that additional reporting requirements will impact funds available for schooling. The need to obtain a level of assurance on interim March 31 statements could have such an impact by increasing audit costs of school districts. Many options have been considered and we will be working with the Office of the Auditor General, as well as the Ministry of Education and school districts, in an attempt to resolve this issue in a mutually satisfactory manner. Such a solution must balance gains in financial statement accuracy against cost.

Financial effects of important decisions on the Summary Financial Statements

The Auditor General's discussion of the financial effects of important decisions primarily provides more background material on items included in the financial statements.

At the end of that section, the Auditor General discusses the current accounting related to BC Hydro. We have raised a concern with the Auditor General that our current policy to reverse the impact of BC Hydro's use of a rate stabilization account may not be in accordance with GAAP. The Auditor General states that in his opinion the current treatment is correct. However, there is a strong opposing argument that will need to be resolved by fiscal 2004/05. When this issue was taken to the independent Accounting Policy Advisory Committee, they recommended that the province should not be reversing the entries of BC Hydro for the rate stabilization account to comply with GAAP.



Part 2:
Computer Systems Supporting Government's Financial Statements

Glossary

Console	A workstation attached to a mainframe system which is used by an operator to enter system level commands that control the operation of the system.
Dataset	A collection of related data items.
Exits	Defined points in computer programs where control is passed from the calling program to a subroutine.
Hotsite	An alternate processing location that has a compatible operating environment that is ready to be activated immediately.
Information	The data digitally stored within the IT Infrastructure.
IT Infrastructure	The hardware, network facilities and software used for the storage, processing and transmission of government information.
Log on	The process by which a user requests and receives authentication from the operating system and is then able to use specific authorized system resources.
Multiple Virtual Storage (MVS) operating system	Refers to the IBM OS/390 operating system.
Privileges	The data and systems functions that a user is allowed to access and utilize.
Read	The ability to look at, or copy, data or systems.
Security Architecture	An overall design of the components that together comprise a whole security structure.
User identification	The means by which a user is uniquely identified to an IT resource, commonly referred to as a user ID, which can be a function of the user's name, an alphanumeric value or a randomly allocated alphanumeric value.

Part 2: Computer Systems Supporting Government's Financial Statements

Introduction

Every day, governments, businesses and individuals rely on computers to capture, process and store millions of pieces of data. In British Columbia, successful delivery of government's programs and services, depends on the reliability, availability and integrity of computer systems.

These computer systems also have an impact on our financial auditing. We have moved increasingly away from extensive and costly transaction-based examinations to more focused, risk-based evaluations. We have been able to do this where we note that government places appropriate emphasis on controls, including those over resources, systems, processes, organizational culture, structure, and tasks. Evaluating the controls over systems supporting government's operations, therefore, can be helpful to us in our audit of the Summary Financial Statements.

Not all systems are reviewed annually. Instead, we plan to cover key systems on a rotational basis and as our resources permit. In an effort to enhance government financial accountability, in this section we report to the members of Legislative Assembly and the public on matters of interest resulting from these reviews. This year, we report on our review of what is referred to as the MVS Environment.

Many government programs, ranging from collecting taxes, to funding health care, to managing our forests, process their data simultaneously on the same central computer. Data from these systems is input to the Corporate Accounting System, reports from which are used to prepare the Summary Financial Statements. This central computer is a powerful IBM mainframe, to which government offices throughout the province are connected. A complex operating system manages these connections and allows data to be processed by numerous end user programs, or applications, at the same time. This operating system, or platform, is called Multiple Virtual Storage, or MVS, and is currently the largest computer platform used by the government of British Columbia. It is also the most important component of the MVS environment.

What is the MVS environment?

The MVS environment includes the operating system, security system, database management software and other software and hardware components that allow the users' applications to process. While it includes everything necessary to enable these applications to run, it does not include the applications themselves. To illustrate the distinction between environment and applications, consider a shopping mall, filled with retail businesses. The mall is the environment that enables individual businesses to operate effectively and efficiently. It provides security and other common services required by the retail stores (the applications) while they perform their function of serving customers (processing). Similarly, the MVS environment provides an infrastructure where computer applications belonging to many users can process information. As the mall can support multiple stores each serving a number of customers, so can the MVS environment support multiple applications with many users.

Background

MVS processing services support a wide variety of mission-critical applications across government. Some examples are the Medical Services Plan's Registration and Premium Billing System and Medical Claims System, Finance's Cash Flow Management System, and Forest's Harvest Database System. Most processing occurs during normal government business hours, but some online systems must be accessible 24 hours a day and able to process critical batch jobs at night. Generally, government users have access to a basic suite of software products, including those for interactive time-sharing, online transaction processing, network connectivity, and batch services.

In May 1998, the Province of British Columbia contracted with IBM Canada Ltd. for the delivery of MVS services. The original contract was for five years, but we understand it has now been extended until July 31, 2006. IBM subcontracted the provision of these services to ISM-BC, which became TELUS Enterprise Solutions (TES) in 2001.

The Information Technology Services Division (ITSD) is responsible for ensuring that the MVS environment is properly controlled. This environment consists of the hardware and

Recently, ITSD was significantly restructured so that it could better support the government's move to shared services. Following the restructuring, ITSD was renamed Common IT Services. However, because the organization was still known as ITSD at the time of our audit, we have used the original name throughout this report.

software used for the storage, processing and transmission of government information. TES is responsible to ITSD for providing and maintaining the environment.

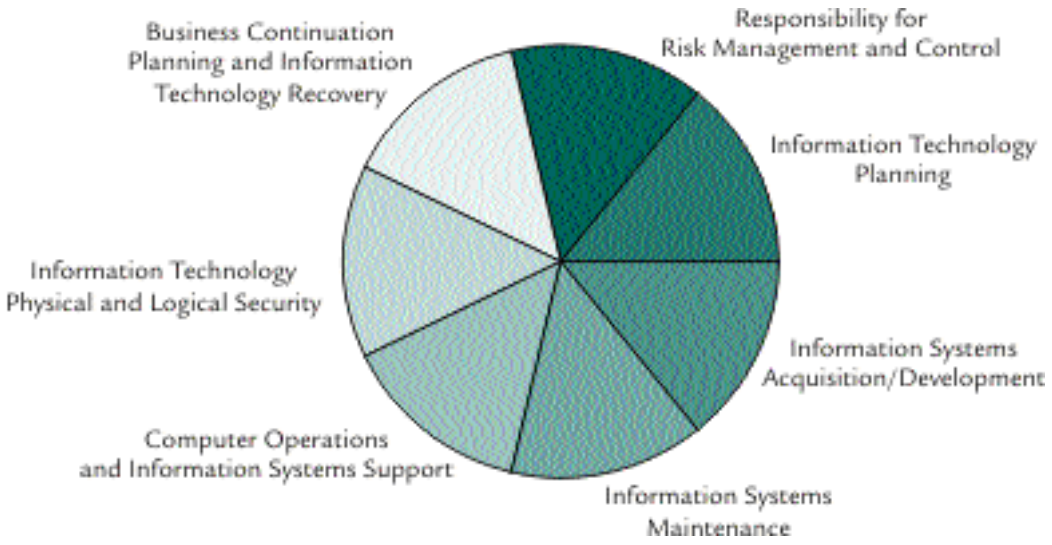
Purpose of the Audit

We were engaged by ITSD to audit the internal control objectives for the MVS environment and the key control procedures designed to achieve those objectives, as they relate to computing services provided to the government of British Columbia at the TES Data Center. Setting these internal control objectives and establishing procedures to achieve them were the responsibility of ITSD management.

The internal control objectives for the MVS environment, were derived from the Information Technology Control Guidelines set out by the Canadian Institute of Chartered Accountants (CICA). These objectives are grouped into categories based on control issues (see Exhibit 2.1). They address the management of risks arising from the use of information technology in an organization,

Exhibit 2.1

Categories of Control Issues addressed in CICA's Information Technology Control Guidelines



and the roles and accountabilities of the people who manage and use information technology. Exhibit 2.2 provides a list of internal control objectives for each control issue included in the audit.

Scope of the Audit

The MVS computing services that TES provides the Province of British Columbia are based in Victoria and Burnaby. A storage facility for back-up tapes is located in a third location, in Victoria.

The mainframe computer installation runs under IBM's MVS operating system. The government is currently processing data on two central processing units (CPUs) with four logical partitions (LPARs) and one Resource Access Control Facility (RACF) database. In this audit, we looked at the system settings for three production LPARs (the one dedicated to testing was not included) and the RACF database.

The security and control of the government applications that reside in the MVS environment were outside the scope of this audit. As well, examination of the data communications network was limited to the interface to the MVS mainframe computer.

We performed our assessment of key control procedures, identified by ITSD and TES management, from November 2001 to January 2002. Our analysis of logical access—that is the ability for a user to read or manipulate data—focused on an extract from the RACF database on November 1, 2001.

Any system of internal control has inherent limitations. This means that, despite the control procedures in place, errors or irregularities may occur and go undetected. Further, projecting an evaluation of a system to future periods is subject to the risk that procedures become inadequate as conditions change or that compliance with procedures deteriorates.

Overall Conclusion

The MVS operating environment is a long-established, stable environment, and has been used in processing government applications for a number of years. However, there is still a risk that security breaches or system failures could occur.

Exhibit 2.2

Internal control objectives for Multiple Virtual Storage processing for the Government of British Columbia

A. Responsibility for Risk Management and Control

- The TES and ITSD corporate cultures support the identification, assessment and management of information technology risk.
- Information technology risk is effectively managed at all levels.

B. Information Technology Planning

- An effective information technology plan that demonstrates the management of risk is in place.
- The overall information technology performance is effectively measured.

C. Information Systems Maintenance

To ensure that systems continue to meet business and technical requirements:

- Controls exist to ensure the authorization, approval, testing, implementation and documentation of changes or additions to the components of the information technology infrastructure.
- Controls exist to protect against accidental or unauthorized changes to the information technology infrastructure.

D. Computer Operations

- Computer operations services at TES and ITSD are appropriately controlled and meet defined user requirements efficiently and effectively.
- Both TES and ITSD ensure the integrity and availability of computer operations services.

E. Information Systems Support

- Systems software procedures and activities contribute to the reliability, effectiveness and control of computer operations services.
- Logical access over network components installed on the host are appropriately controlled.

F. Information Technology Physical and Logical Security

Access Controls

- Controls are in place to ensure the integrity, confidentiality and availability of information technology processing throughout the organization.
- Logical access to systems and information is reliably controlled.

Facility Controls

- The information technology resources are housed and operated in appropriate environmental conditions.

Personnel Controls

- Appropriate consideration is given to technical skills when management and staff are hired into information technology positions.
- Appropriate consideration is given to security issues when management and staff are hired and terminated.

Security Policies and Procedures

- Information technology security is operated in an efficient and effective manner.

G. Information Technology Back-up and Recovery

- Critical information systems processing functions can be resumed promptly in the event of significant disruption to normal computer operations.

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.

We found that all of the control procedures identified by ITSD and TES management were suitably designed to meet the control objectives, and we found that most procedures existed. However, we identified a number of cases where actual practice did not comply with the stated control procedures, indicating that the level of risk was greater than management intended. Most of these cases related to access by ITSD and TES staff to system files, commands, functions and government information, when such access was not necessary for the staff to carry out their duties. Such access allows the staff member to make changes to the system, to read government data, and to change logs recording activity in the system.

We also found that a very small number of external users had on-line access to the system rather than restricted batch access. This meant that it was possible for these users to gain access to government information.

As a result of the weaknesses found, we concluded that not all of the control objectives were met. Details of the weaknesses, organized under each internal control objective, are found in the detailed findings of this report.

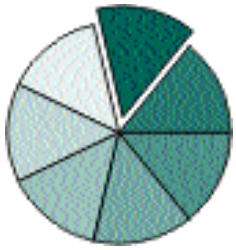
We received full information and wholehearted cooperation from the management and staff of TES and ITSD during the course of our audit.

Detailed Findings and Conclusions

We present our findings and conclusions below, organized under each internal control objective described in Exhibit 2.2.

Security considerations are a crucial element of control over Information Technology, and are at the root of many of the control procedures addressed here. As well, security is specifically examined and reported in its own part of this report (Section F).

A. Responsibility for Risk Management and Control



Risk is the chance of something happening that will have an impact on the control objectives, creating an irregularity in the computing environment. Risk management takes in the identification of the risk, the assessment of the impact of that risk, and the determination of the level of control necessary to minimize that impact. The cost of implementing and maintaining control is balanced against the potential cost of the negative effect.

Corporate Culture

Control Objective

The TES and ITSD corporate cultures support the identification, assessment and management of information technology risk.

Control Procedures

1. Policies and procedures exist to inform new and current employees of information technology risk.
2. Policies and procedures stress the importance of risk management and are reinforced throughout the organization.

Conclusion

The control culture in any organization has a significant impact on whether information technology risk is appropriately managed. We found that both TES and ITSD captured the importance of information technology risk in their policies and procedures and are communicating it to new and current employees.

The control procedures were suitably designed and existed at the time of our audit.

Management of Risk

Control Objective

Information technology risk is effectively managed at all levels.

Control Procedures

1. Responsibilities for the establishment of policies and procedures are defined, within ITSD and TES, for the protection of the information technology infrastructure and information.

2. Supervisory positions exist to monitor the extent to which development, operation and control of the information technology infrastructure and information complies with established policies and procedures.
3. Specific security functions exist with responsibilities for developing, maintaining and ensuring ongoing compliance with security policies and procedures.
4. A contract outlines the ownership of each information technology service.
5. Job descriptions and policies outline responsibilities.
6. Audits of security access are done every six months for each department to ensure responsibilities are still relevant and are reviewed.

Conclusion

Effective risk management requires support and participation from all levels of an organization. Both ITSD and TES have defined who is responsible for establishing policies and procedures to protect the information technology infrastructure and information. The extent to which the development, operation and control of the information technology infrastructure comply with these established policies and procedures is monitored.

The control procedures were suitably designed and existed at the time of our audit.

B. Information Technology Planning

The integration of information technology initiatives with the strategic business plan is critical. An information technology plan helps an organization manage risks such as excessive costs, inadequate performance, unpredictable processing and lost opportunities.

The Information Technology Plan

Control Objective

An effective information technology plan that demonstrates the management of risk is in place.

Control Procedures

1. TES has established policies and procedures to ensure that the terms of the contract with the Province are fulfilled.
2. Responsibilities have been assigned to carry out established policies and procedures.
3. For government, TES conducts a yearly planning session, taking into consideration what was done during the past year (including accomplishments) and what will be done next year (projects and objectives).

Conclusion

We found ITSD to be exercising its information technology plan through its contract with TES.

The control procedures were suitably designed and existed at the time of our audit.

Information Technology Performance Measurement

Control Objective

The overall information technology performance is effectively measured.

Control Procedures

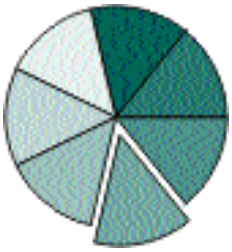
1. Weekly and daily capacity / usage reports are produced and reviewed.
2. TES reviews the reports on service levels, compares the findings to the contract and reports to the Province.
3. Annually, TES assesses MVS capacity and appropriate plan modifications are agreed on with the Province.

Conclusion

Developing the information technology objectives, strategies and plan is the first stage in the planning process. Monitoring their implementation and effectively using the results are equally important. We found that the overall performance of information technology was being effectively measured.

The control procedures were suitably designed and existed at the time of our audit.

C. Information Systems Maintenance



The goal of information systems maintenance is to maintain and modify systems so that they can meet user needs on an ongoing basis. Procedures related to this task should ensure that only authorized changes, duly tested and documented, can be implemented. Proper control over the maintenance process ensures that the MVS operating environment continues to meet business and technical requirements.

Management of Planned Changes

Control Objective

Controls exist to ensure the authorization, approval, testing, implementation and documentation of changes or additions to the components of the information technology infrastructure.

Control Procedures

1. A formal approval process exists for making any changes to the information technology infrastructure. The process includes procedures such as:
   - Approval of the owner before a change is initiated.
   - Use of a standardized change request form, which describes the nature of and reason for the change and is approved by a designated manager.
2. "INFOMAN," a change control tool, provides procedures for change management, and "Remedy" provides procedures for problem management. Together they provide the following functions:
   - Change request initiation and status,
   - Change approval, and
   - Problem request initiation and status.
3. Changes are recorded electronically, along with approvals, creating a management trail of changes.
4. The responsibilities for initiating and approving system software changes are properly segregated. Review and approval of system software changes are required from appropriate TES staff, including the Change/Problem Management Manager.

5. The Change/Problem Management Manager reviews all system software change requests for proper approvals and determines whether the implementation and test plans (including procedures to go back to the original state) are adequate for the nature and risk of the proposed change.
6. Where appropriate, changes are accompanied by updates to documentation, updates to the help desk, and updates to operational procedures.
7. All information technology infrastructure changes are documented. Documentation includes change history, customer authorization, TES approvals, test plans and results, implementation instructions, and back-up plans.
8. Technical Information Bulletins are produced to advise users of upcoming changes and their effect on processing.
9. Vendor-recommended installation utilities, when available, are used to install system software changes, and changes are performed in accordance with vendor instructions.
10. Changes to system software are tested in the customer test/development system before they are implemented in the production environment.
11. Information technology infrastructure changes are implemented during the standard change window.
12. MVS staff sends a note to ITSD security when changes occur or are planned. TES makes most changes through the SPIN process. These are reviewed with ITSD for approval and implementation.
13. Weekly change meetings are held involving the Change/Problem Management Manager and technical services staff.
14. Reports are prepared on a regular basis showing planned changes and the status of changes, for review by information systems management.
15. Emergency changes follow the same process and controls as are used for other system software changes, except the time frame is compressed and the documentation and approvals may not be completed until after the fact.

16. There are back-up procedures for restoring previous to changes.

17. ITSD sends a list to TES outlining the emergency changes that have happened or changes to be implemented. This gives the department heads a chance to note any problems.

Conclusion

When the ITSD and TES data centres merged, a new process was implemented for managing software changes on the MVS platform. The "SPIN process" involved building a base system and then adding customizations unique to ITSD requirements. This establishes a common and consistent support structure to maintain, support and upgrade MVS. Many of the control procedures are part of this process.

The control procedures were suitably designed and existed at the time of our audit.

Preventing Accidental or Unauthorized Changes

Control Objective

Controls exist to protect against accidental or unauthorized changes to the information technology infrastructure.

Control Procedures

1. Data is protected through the use of the Resource Access Control Facility (RACF) to ensure that only authorized personnel are able to perform changes on the data.

2. The change control process requires that the resource owner agrees before the change goes ahead.

3. Access to system software libraries or directories is restricted to the appropriate TES system support staff and ITSD Security Services by RACF.

4. Activity related to key production system software datasets is recorded by RACF.

5. Standards require that all new or previously installed products in the government environment either interface with RACF or have an exit developed that meets security requirements (access to government files must be authorized) before implementation.

6. MVS and related IBM and third-party software products are implemented using the System Modification Program.

7. There is proper segregation between systems development, systems testing, systems support and computer operations.

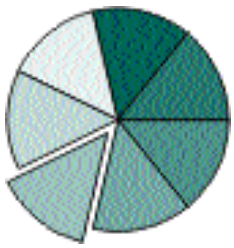
Conclusion

To ensure that only authorized personnel are able to perform changes, production system software and data are protected through the use of RACF. The following deficiencies in control procedures existed. These are further discussed under control procedures described under "D. Computer Operations."

- There is proper segregation between systems development, systems testing, systems support and computer operations, however we have noted a control deficiency regarding the segregation of duties related to the use of operator commands.
- Access to system software libraries and directories was not restricted to only appropriate system support staff by RACF.

We therefore concluded that the control procedures were suitably designed, and except for the two noted above, existed at the time of our audit.

D. Computer Operations



The mainframe computer installation runs under IBM's MVS operating system which, with its subsystems, schedules the processing of programs, monitors the activity within the system, and coordinates and controls other hardware devices such as terminals, tape and disk drives, and printers. There are inherent risks in computer operations, such as inaccurate or unauthorized processing, loss of systems availability and loss of confidentiality of information or systems.

Meeting User Requirements

Control Objective

Computer operations services at TES and ITSD are appropriately controlled and meet defined user requirements efficiently and effectively.

Control Procedures

General:

1. Operations and support service levels provided by TES are outlined in the contract with the Province.
2. TES keeps up with the supported version of hardware and software. Exceptions to the rule have a valid reason for being that way.
3. Automated tape management systems are implemented to provide standard tape inventory management controls, file / data identification controls, and expiration dates and retention criteria.

System logging:

4. An automated system is used to record all system activity.
5. There are controls over the completeness, accuracy and integrity of logs that are relied on to record system or operator activities. Access to log files of the System Management Facility (which records who uses the system) is restricted by RACF.
6. Key System Management Facility record types for audit, control and security usage are recorded.
7. There are procedures in place to ensure the timely dumping of the System Management Facility files to prevent data loss.
8. The System Management Facility dump program is executed from a write-protected library.
9. System Management Facility exits, which are active in the system and can be used to alter system processing, are properly documented and controlled.
10. Operators are not allowed to change individual System Management Facility parameters.
11. Automated techniques are used to analyze system logs.
12. Management, involved with information systems processing, review reports produced from the analysis of the system and manual logs.
13. RACF controls access to utility programs.

Problem identification and resolution:

14. Systems tools are used to automate operations and to identify and recover from operating errors.
15. Vendors have access to the system to monitor the hardware, software and storage media for any errors.
16. Escalation procedures have been clearly defined.
17. Similar procedures to those used for Change Requests are used for Problem Management. Problems requiring a change to the production environment are initiated as Change Requests.
18. Periodic maintenance of hardware and systems software is performed according to vendor specifications.
19. There is automatic robotic tape cleaning.
20. Direct Access Storage Device usage is monitored on a regular basis. Disk space reorganization and clean-up is performed regularly.
20. Service level reports are produced and tape mount levels are measured.

Conclusion

We found several problems:

- The controls over the completeness, accuracy and integrity of logs that are relied on to record the system activities were not adequate. A number of support staff had access levels greater than required, creating a risk that the log that records hardware and software error information and the log that records operator actions may be inaccurate or incomplete.
- The System Management Facility records the use made of the system's resources by individual users, providing a management trail for the system. Some support staff had inappropriate access to the program that routinely saves the System Management Facility log records to files, creating a risk that the management trail for the system may not be accurate or complete.
- The System Management Facility exits, which are subroutines that can be used to alter system processing, could be accessed by some support staff who do not require the access.

We therefore concluded that the control procedures were suitably designed, and except for the three noted above, existed at the time of our audit.

Ensuring the Integrity and Availability of Computer Operations

Control Objective

Both TES and ITSD ensure the integrity and availability of computer operations services.

Control Procedures

General:

1. Procedures exist to support day-to-day operating activities (including shut-down procedures, and restart and recovery procedures).
2. Documented procedures exist for data resource management and computer operations.
3. Documented procedures exist for production scheduling and control.
4. Software is used to the extent possible to reduce the number of discretionary manual procedures required, and to monitor the performance of manual procedures. Console operations and application scheduling are highly automated for all routine processes.
5. For batch jobs submitted by and under the control of TES, procedures exist to ensure only authorized jobs are included in the job schedule.

Problem identification and resolution:

6. Procedures exist for adequate problem identification, resolution and reporting of system failures, restart and recovery, emergency situations, and other unusual situations.
7. Daily meetings are held to review and analyze operations problems and their resolution. These meetings include all key personnel affected.
8. Operator actions in the event of incidents are reviewed for appropriateness and to ensure the results of processing are not adversely affected.

9. The automation of batch flows alerts staff of an event occurring and procedures for each event are in place and documented online.

10. Monitoring occurs 24 hours a day, 7 days a week.

Segregation of duties:

11. The privilege to issue operator commands is adequately controlled and reviewed regularly.

12. Command Centre Shift Supervisors supervise activities of operations personnel.

13. Approval, including user involvement where appropriate, is required for variations in parameters and control statements that might affect the way a batch job or an online system runs, and for departures from authorized set-up/run procedures.

14. Standard change management procedures exist to move revised production applications from the test area to production.

Job scheduling:

15. Job scheduling systems (ESP) are used to automate the submission of batch jobs. The scheduling product requires that documentation be prepared for each job implemented into ESP.

16. Job scheduling systems ensure that the application production environment is appropriately controlled.

    - The datasets of the job scheduling system, ESP, are secured by RACF.
    - The appropriate ESP general resources are defined to RACF to protect access to ESP.
    - Security rules are defined under RACF to protect access to ESP procedures and the use of ESP commands and functions. Access is restricted to appropriate personnel based on functional responsibilities.

Tape library:

17. There is a tape librarian function at the data centre.

    - Procedures exist within the tape library to ensure the integrity of files.

- The tape management system, IBM's Data Facility Systems Management Storage (DFSMS), is protected by the operating system security (RACF) and/or external access control software.
- The appropriate DFSMSrmm, the removable media management component of the DFSMS, general resources are defined to RACF to protect access to DFSMSrmm.
- Security rules are defined under RACF to protect access to DFSMSrmm commands and functions. Access is restricted to appropriate personnel based on job responsibilities.
- DFSMSrmm provides functionality to ensure that the correct volumes and datasets are used.
- Cataloguing procedures and standards are enforced.
- All tapes have external labels. Access to non-labelled tapes is controlled by RACF.
- DFSMSrmm has the standard control features implemented, including:
  - tape dataset identification controls
  - expiration dates and retention criteria
  - interface with RACF
  - logging of catalogue changes for restoration
  - multiple-volume/multiple-file processing
- Removal of tapes from the tape library must be authorized.
- DFSMSrmm inventories tape files used by operations.
- Use of bypass label processing is restricted.

MVS configuration:

18. Procedures exist for setting up batch jobs and the initial loading and subsequent use of system software, including dynamic changes to and maintenance of system parameters.
19. All government production jobs initiated or run by TES are authorized by the appropriate customers.
20. Defined control procedures exist for the implementation of Program Temporary Fixes and Authorized Program Analysis Report and user modifications.

MVS Configuration

The MVS environment is complex and much of the integrity of the MVS environment depends on the control over the MVS system configuration and system libraries. Access must be restricted to appropriate personnel and any changes approved and subject to proper change control procedures. Critical components of the system have been examined and are described below.

- The PARMLIB is the library that contains the parameters for building the system during an Initial Program Load. The settings affect performance, security and exposure to sensitive data.
- The Program Properties Table is a MVS function that will automatically grant programs special powers to run. Usually this involves back-up and recovery programs that need to access files without knowing the password, or programs that need to override exclusive control.
- The Authorized Program Facility is a mechanism in MVS software that enables programs to place themselves in "supervisor state," thereby bypassing IBM's system integrity and enabling the use of special operating system functions.
- The Master Catalog contains dataset and volume information necessary to locate datasets and user catalogs. It is read during a system initialization and is vital to the functioning of MVS.
- Exits are defined points in computer programs where control is passed from the calling program to a subroutine. The functions programmed into the subroutine are performed and completed before control is returned to the same exit point. Exits are intended to be user customizable and allow the data center to add functionality to the system without changing the system source code. Many exits run in an authorized state with the ability to bypass security.
- User Supervisor Calls (SVCs) are special routines that enable a normal, non-authorized task, to perform a system level task. To execute a SVC, a program will call the SVC. The SVC will assume control and execute the task, then return control to the initiating program. SVCs are very powerful because they run in supervisor state. They also create a source of possible security exposures to the operating system because the calling program has control in supervisor state.
- Job Entry Subsystem (JES2) is software that controls the execution of all jobs and manages the output from those jobs. JES2 schedules jobs for execution, manages the spools that contain output before and during printing, and manages printers. JES2 can be customized through parameters.
- IBM provides a set of general-purpose MVS utility programs. The utility programs provide a convenient method of performing such tasks as deleting, renaming, cataloguing, uncataloguing, moving, copying, merging and modifying datasets.
- Started tasks are subsystems such as JES, CICS and IMS, that are always running and available for user requests. They are run under a user ID which should be dedicated to the task and therefore, protected from being revoked or being used by an individual.

21. Access to the production PARMLIB datasets is restricted to appropriate personnel. Changes to all production PARMLIB datasets are approved and subject to change control procedures.

22. The contents of the Program Properties Table reflect standard IBM and appropriate installation-defined entries. Changes to Program Properties Table entries are approved and subject to change control procedures.

23. Security rules are defined under RACF for each Authorized Program Facility (APF) library and access is restricted to appropriate personnel.
24. Access to the MVS Master Catalog is restricted to appropriate personnel.
25. Changes to exits are documented as to purpose and function. Standard IBM documentation is maintained for all MVS exits. Implementation of exits into the production environment is properly approved and subject to change control.
26. User Supervisor Calls (SVCs) are documented as to function, usage and operation. Standard IBM documentation is maintained for all IBM SVCs. Access to SVC source and load libraries is appropriately restricted.
27. Job Entry Subsystem (JES2) software options are appropriately set. Changes to JES2 options are approved and subject to change control.
28. Utility programs, which have the capability of bypassing the access control mechanism, can only be executed from protected libraries. Access to utilities is restricted to appropriate personnel.
29. Started tasks (STCs) are protected by ID association. Associated IDs have access to the STC only, have no online access authority, and are provided with secure passwords.

Computer output:

30. Computer output is produced in a secure area.
31. RACF controls logical access to the output on the spool.
32. Procedures exist for record destruction and handling, and facilities are provided for disposing of sensitive documentation and media.

Back-up tapes:

33. Logical access to back-up tapes is secured by RACF.
34. Disaster Recovery Planning (DRP) testing does check the back-up.

Conclusion

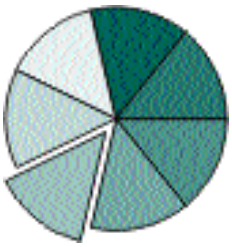
We found several problems:

- Support staff from several departments were able to issue all operator commands, yet there was no regular review of the issuance of the commands. This creates a risk that operator commands can be used inappropriately, resulting in data security, system security or system performance being compromised. Management told us that it would not be operationally efficient to have all commands issued through operators. However, given the security and performance risk that these commands could generate, and the lack of other controls protecting the commands, we believe access should be granted only to users who have a specific reason to issue these commands.
- Security rules are defined under RACF to protect access to DFSMSrmm commands and functions. However, a number of support staff had access to some DFSMSrmm commands and functions, even though they did not require it. The access would allow individuals to perform such actions as deleting the data on a tape, thus risking loss of data integrity and confidentiality.
- Inappropriate support staff had the ability to create non-labelled tapes. This, in our view, puts the integrity of government information at risk.
- Use of bypass label processing is restricted, but there existed inappropriate access to the facility that controls the use of bypass label processing. This created a risk that the integrity and confidentially of data files could be compromised.
- Although security rules were defined under RACF for each Authorized Program Facility (APF) library, there was excessive access by a number of support staff to the commands that could enable programs to become APF authorized.
- The Master Catalog, which contains information to allow all data to be located, was write-accessible to a number of support staff. Inappropriate access to the Master Catalog could result in unauthorized changes to or destruction of the catalog, which would compromise the security and performance of the system.
- Supervisor Call libraries, containing programs that communicate with the operating system, were accessible to an inappropriate number of support staff. This access could compromise operating system security.

- Utility programs, which have the capability of bypassing security controls, should be executed only from protected libraries. All MVS users had "execute" access to a utility that could overwrite tape labels, regardless of the security protection on the tape.
- Many started tasks were running under user IDs that were unprotected. This created a risk that the subsystems could be stopped if the user ID was revoked. We also found that some of these user IDs had online sessions, meaning that if someone was able to log on with the ID, he or she would also gain access to many other resources.
- A number of support staff had the capability to either read, copy or delete a significant number of back-up tapes. Those excessive access capabilities could result in unauthorized retrieval of government information from the tapes.

We concluded that the control procedures were suitably designed. Due to the deficiencies noted above, eight control procedures did not exist at the time of our audit.

E. Information Systems Support



System software is integrated with business applications, providing functionality such as database management. Changes to the system software settings could significantly impact the business. Also, the configuration of the network can result in benefits or risks to the security and control of the organization, depending on the way that settings are established. Therefore, changes to system software settings need to be properly managed and controlled.

System Software Procedures

Control Objective

Systems software procedures and activities contribute to the reliability, effectiveness and control of computer operations services.

Control Procedures

1. Vendor instructions and recommended configuration settings are adhered to unless there is an explicit need for customization.
2. Hardware and software performance is monitored and compared to industry benchmarks.

3. Products are evaluated on functionality and pricing, and requests for proposals are issued depending on the dollar amount and the selection of products (if there is a choice).
4. Any PC attaching to the TES network has an anti-virus protection program. TES has standardized on McAfee.
5. The security departments in TES and ITSD are pro-active in addressing viruses.

Conclusion

We found that the system software procedures and activities being used by TES and ITSD were providing reliable and effective control over computer operations services.

The control procedures were suitably designed and existed at the time of our audit.

Logical Access to Network Components

Control Objective

Logical access over network components installed on the host is appropriately controlled.

Control Procedures

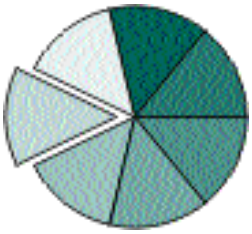
1. Access to the MVS environment is authorized by RACF.
2. Critical network and systems software components and subsystems have been configured to utilize the security provided by the operating systems and/or external access control software.
3. Access to network and system software files/datasets is restricted to the appropriate staff.
4. Access to network and system utilities is restricted to the appropriate system support staff.

Conclusion

Some support staff inappropriately had the ability to change or delete network system files. This creates a risk that system performance could be negatively affected.

We concluded that the control procedures were suitably designed, and except for the one noted, existed at the time of our audit.

F. Information Technology Security



Information technology security should be a balance between enabling staff to access information and systems easily and efficiently, and controlling the access that is permitted. Security requirements can be communicated through the implementation of a security architecture that defines the organization's overall approach to security, including policies and procedures, awareness programs and compliance monitoring.

Integrity, Confidentiality and Availability of Information Technology Processing

Control Objective

Controls are in place to ensure the integrity, confidentiality and availability of information technology processing throughout the organization.

Control Procedures

Organizational framework:

1. Procedures exist within TES to provide an organization-wide security architecture.
2. TES has defined and implemented security policies that describe: the assets to be protected; management and employee responsibilities for protecting the assets; and TES's intention to enforce its security policies.
3. The security policies have received approval from the Vice-President, Operations.
4. The Vice-President, Operations is responsible for establishing security policies and standards and for ensuring compliance with and achievement of policy.
5. Each TES employee must read and adhere to the company's Business Conduct Guidelines.
6. TES employees must sign a confidentiality agreement.

Assignment of responsibilities:

7. An owner is assigned to all resource types (i.e. development programs, production programs, production datasets, and system datasets) to ensure that all actions affecting a resource are reviewed by the appropriate person.

8. Data owners are responsible for the classification of the data. The custodians' responsibility includes the exercising sound business judgement, complying with applicable directives and agreements, and administering owner-specified business and asset protection controls. The owner of the data decides whether it is confidential (ITSD responsibility).

9. Security functions exist within the TES Operations Division with responsibility for developing, maintaining and ensuring ongoing compliance with comprehensive security standards and procedures.

10. TES is divided into a number of divisions, one of which is Operations. The Operations Division (which is primarily responsible for maintaining the government MVS environment) is divided into a number of departments and responsibility areas, each of which has distinct and separate responsibilities.

11. Management of TES assigns responsibilities to each functional group responsible for information technology administration and operations. Function responsibilities and reporting relationships are defined and communicated.

12. Each functional group's responsibilities are segregated. In particular, data centre operations, system software support, physical and logical security and monitoring, application software development and maintenance, change management and help desk functions are segregated.

13. Job descriptions outline responsibilities for each position.

14. Positions exist within each service delivery area of the organization to provide adequate supervisory control.

15. Data for the ministries is segregated and an approval process must be followed for TES to get access.

16. The appropriateness of TES access to the government-computing environment is reviewed every six months.

17. Vanguard and RACF courses, conferences, seminars and user training sessions (in ESP, for example) are conducted.

Conclusion

The control procedures were suitably designed and existed at the time of our audit.

Logical Access to Systems and Information

Control Objective

Logical access to systems and information is reliably controlled.

Control Procedures

User IDs and passwords:

1. Standard procedures exist for requesting the establishment of new user ID accounts and additional access capabilities.
2. Standard procedures exist for assigning and controlling passwords. All users are assigned unique user IDs and all IDs are assigned a password.
3. Passwords are changed every 40 days for MVS user accounts. Procedures exist to suspend or temporarily deactivate (revoke) user accounts in the event of specified unsuccessful access attempts. As well, procedures exist to automatically revoke access for user IDs that are inactive over a specified period of time.

   3a. Non-expiring passwords have been enabled for non-government users where application owners have requested and approved its use based on specific documented business needs. The following procedures exist:

   - User IDs are revoked after three invalid password attempts.
   - User IDs are automatically revoked after 90 days of inactivity.
   - User IDs are restricted to "Inquiry Only" access.
   - Authority to reset forgotten passwords is restricted to the local security contact or a central Help Desk.
   - Authority to resume revoked user IDs is restricted to the local security contact or a central Help Desk.
   - The local security contacts routinely revoke the user IDs of individuals who leave their organizations or change responsibilities and no longer require access.

- Users are able and encouraged to change passwords if they wish or as required.
- Information is provided to users to assist them in the selection of secure passwords.
- A non-expiring password is set at the individual user ID level, not globally.

3b. The use of non-expiring passwords is restricted to machine-to-machine connectivity and to user IDs that have been granted this condition based on ITSD's acceptance of the users' documented business needs. These exceptional user IDs are subject to the following RACF rules:

- The user ID will be disabled after three unsuccessful attempts.
- The user ID will be revoked after 90 days of inactivity.

4. Access by ITSD and TES users is reassessed when their job function changes and deleted immediately upon their employment termination.

5. The operating systems and the external access control software (RACF) have been properly implemented (with appropriate security options and parameters) to provide users with the capability of securing data, applications and systems resources. Write-access to system software files is restricted to TES employees according to job responsibilities. Individual accountability can be determined when such access is made. Access to government data and program libraries by TES employees is also restricted according to job responsibilities. Individual accountability can be determined when such access is made.

Security Administrators:

6. A separation exists between the security administrators and the data processing area in terms of reporting structure and job responsibilities. Only authorized individuals have security administration capabilities. Individuals with security administrator user IDs do not have access to any resources except those required to perform their job function.

7. RACF allows access through the assignment of group and individual profiles. Management performs an evaluation of access assignments to ensure they are still appropriate. In particular, an independent review of the security administrators' actions is performed.
8. The group data security administrator structure effectively controls and manages ownership of RACF profiles.
9. RACF interface is installed for the critical system software components.
10. System-wide RACF control options are set to provide an acceptable level of security.
11. Access to the "special" and "operations" attributes is restricted according to job responsibilities.
12. The global access table is only used for system-wide resources, based on a business need.
13. Access to the RACF database and its back-ups is highly restricted.
14. Changes, deletions and additions to the RACF database are made through appropriate procedures and adequately supported by approved documentation.
15. RACF control options are not changed without appropriate authority. Access to change RACF options is appropriately restricted.

Customer Information Control Systems (CICS) regions:

16. Parameters to provide a RACF interface with the CICS regions are set. Security rules are defined under RACF and CICS to protect access to CICS transactions.

Database 2 (DB2):

17. Parameters to provide a RACF interface with the DB2 are set. DB2 is set up in the RACF DSNR general resource class.

Information Management System (IMS):

18. Parameters to provide a RACF interface with IMS are set. The APIMS general resource class is defined to RACF to protect access to IMS applications.

Emergency user IDs:

19. Emergency user IDs have been assigned access to the appropriate resources. Adequate controls are in place for the release and revocation of emergency user IDs. Sensitive resources that are controlled by emergency user IDs are restricted from other users. Activity performed through the use of emergency user IDs is logged, documented and reviewed by management.

Security access logs and reports:

20. Key security events or violations in the Network and MVS environments are logged. Security Services staff review and investigate key security events, such as successive violations to critical resources and invalid access attempts. Security violations of any serious nature are sent to senior management and recorded and filed as security incident records. Access and access violation reports are generated on a daily and weekly basis and made available to government and TES management. Weekly security reports are reviewed and appropriately investigated and followed-up by ITSD security personnel. The security personnel also advise government clients of unprotected datasets identified in the weekly reports.

Logical access audits:

21. Internal audit at TES monitor security administration on a regular basis. Approximately every six months, Lotus Notes is used to audit whether a person still works on the same job and needs the same access.

    The retention period for the System Management Facility records, which is the source for RACF information, is one year.

    The use of user IDs with the "special" attribute is audited by RACF and reviewed by TES and ITSD.

    RACF audits all access to datasets where access is granted because the user ID has the "operations" attribute.

22. A tape management system is in place to control access to tape volumes.

Conclusion

The Resource Access Control Facility (RACF) provides the ability to identify and authenticate users, authorize users to access resources and record and report unauthorized access attempts. Access control information about users, groups of users, datasets, and general resources defined to RACF is stored in the RACF database.

Logical access to the system is restricted by the requirement of a unique user ID and password. The authentication of the user through the unique user ID and password combination ensures personal accountability. Standard procedures exist for requesting the establishment of new user ID accounts and additional access capabilities and for assigning and controlling passwords.

Responsibility for security administration has been assigned to ITSD Security Services and the TES Security group. Group Data Security Administrators (GDSAs) represent the users in TES, ITSD, ministries and public bodies. Generally, the security administrators should not perform any other data center duties which could result in a segregation of duties conflict.

We found several problems:

- Where non-expiring passwords have been enabled for non-government users, the user IDs are to be restricted to "Inquiry Only" access. Two user IDs had access capabilities greater than "Inquiry Only," creating an increased risk of unauthorized access to the system through a non-government user ID.
- Several government user IDs had—contrary to ITSD policy—non-expiring passwords and on-line access.
- Support staff had inappropriate access to government data and program libraries, creating a risk of unauthorized access to government information.
- Several staff responsible for data processing also had system-wide security administration capabilities. This creates a risk that unauthorized activities may be performed.
- The evaluation of access assignment was not being adequately performed. In several instances, support staff were granted excessive access to system files and government information.

- Access to the "special" and "operations" attributes was, in some instances, inappropriately granted. This creates a risk that users may inappropriately alter system components or improperly use their authority to circumvent RACF.
- Access to the RACF database was excessive. This creates a risk of unauthorized access to security information defined in RACF. The potential for inappropriate changes, deletions and additions to the RACF database also creates a risk that a user may be given unauthorized access to system resources or government information.
- Access to RACF options was not appropriately restricted. Improper changes to RACF control options may result in unauthorized access to various data resources, including government data, and the possible destruction of government information. All system-wide RACF control options, except logging of security information, can be activated and deactivated by users with the "system special" attribute. We discussed earlier our concern about the appropriateness of the users who have access to "special" at a system level.
- Government programs in the Customer Information Control Systems regions were not adequately restricted to prevent unauthorized users from gaining access.
- Access granted to one RACF group had been building up over a number of years and was excessive. The access extends to government applications and data files processed in Information Management Systems. In our view, if systems support staff are granted access to assist in a support capacity, that access should be revoked once the task is complete.

We concluded that the control procedures were suitably designed. Due to the deficiencies noted above, ten control procedures did not exist at the time of our audit.

Facility Controls: 4000 Seymour Place, Victoria

Control Objective

The information technology resources are housed and operated in appropriate environmental conditions.

Control Procedures

Physical security:

1. Commissionaires in the ITSD Security Services group use closed-circuit TV cameras to monitor the outside of the 4000 Seymour Place building 24 hours a day, and they perform a series of patrols each day.
2. Access in and out of the 4000 Seymour Place building is controlled and monitored by the commissionaires.
3. Individuals must display an appropriate identification badge or cardkey before access is granted to the 4000 Seymour Place building.
4. Procedures are in place to control the issue of identification badges and cardkeys and to safeguard unissued cardkeys.
5. The 4000 Seymour Place building is divided into access zones. Access to each zone is restricted to authorized individuals through the use of an access control system.
6. The access control system logs all unauthorized access attempts to access zones. When an alarm is triggered, a commissionaire investigates.
7. Security incidents are logged by a commissionaire and reviewed by the Physical Security Officer daily.
8. Standard emergency procedures, documents and checklists are available at TES and ITSD to provide assistance to the commissionaires and staff.

Protection from fire and environmental damage:

9. Fire detection and suppression devices are installed in the data centre and in the rest of the building.
10. Moisture detectors are installed in the data centre area.
11. Three water chillers with redundant capacity are installed in the data centre area to cool the computer equipment.

Back-up power:

12. Redundant power supply is available to support the data centre processing and communications equipment.

13. A battery back-up supports the internal telephone system, and telephone and radio devices are available for use in the event of an emergency.

Conclusion

The control procedures were suitably designed and existed at the time of our audit.

Facility Controls: Burnaby Data Centre

Control Objective

The information technology resources are housed and operated in appropriate environmental conditions.

Control Procedures

Physical security:

1. A security guard controls all access to the data centre.
2. A cardkey access system controls access to the command centre and to the areas within the data centre, based on an individual's job responsibilities.
3. All visitors to the data centre must be approved by an authorized TES employee who signs a log retained by the security guard.
4. Formal procedures exist to authorize and maintain card access rights to TES's facilities.
5. Video cameras and security guards monitor all data centre fire exit doors.
6. Active operator consoles are located in secure areas.
7. No physical operator consoles are located outside the command and data centres.
8. An Uninterruptible Power Supply (UPS) system is linked to the doors leading to the data centre to provide operation during power failures.

Protection from fire and environmental damage:

9. A Halon gas fire extinguishing system, which operates automatically on detection of a fire, protects the data centre. Smoke and heat detection devices, which automatically trigger the Halon system, have been installed under the ceilings and below the raised floors of the data centre. These devices are directly connected to the data centre alarm system, which alerts building security, the TES Provincial Network Operational Centre located at a remote site, and the local fire department. The Halon fire extinguishing system and the detection devices are maintained and inspected on a regular basis.
10. Portable fire extinguishers are strategically placed throughout the data centre and inspected on an annual basis.
11. Moisture detectors and drains are located under the raised floor in the data centre near the air conditioning units.
12. The data centre has drainage beneath the raised floors.
13. The data centre has air conditioning and humidity control systems independent of the rest of the building.

Back-up power:

14. Electrical power supply for the facility is protected by redundancy of equipment, including an alternate connection to BC Hydro, duplicate UPS equipment, and several diesel generators.
15. The power supply system is maintained and inspected on a monthly basis.

Conclusion

There is no government CPU or disk room in the Burnaby Data Centre; however key departments such as computer operations and change management are located there.

The control procedures were suitably designed and existed at the time of our audit.

Facility Controls: Back-up Facility, Victoria

Control Objective

The information technology resources are housed and operated in appropriate environmental conditions.

Control Procedures

Physical security:

1. Access in and out of the TELUS building is controlled and monitored by access card readers.
2. Individuals must use an appropriate cardkey before access is granted to the building.
3. Procedures are in place to control the issue of identification badges and cardkeys and to safeguard unissued cardkeys.
4. The building is divided into access zones. Access to each zone is restricted to authorized individuals through the use of an access control system.
5. The access control system logs all unauthorized access attempts to the access zones.
6. Standard emergency procedures, documents and checklists are available to provide assistance to staff.

Protection from fire and environmental damage:

7. Fire detection and suppression devices are installed in the back-up centre and in the rest of the building.
8. Water chillers with redundant capacity are installed in the building to cool the computer equipment in the back-up facility.

Back-up power:

9. Redundant power supply is available to support the data centre processing and communications equipment.

Conclusion

The control procedures were suitably designed and existed at the time of our audit.

Personnel Controls: Technical Skills

Control Objective

Appropriate consideration is given to technical skills when management and staff are hired into information technology positions.

Control Procedures

1. Prospective employees are required to submit a resume with references.
2. New employees are screened during the interviewing process to determine their suitability.
3. Hiring and promotions are indicative of the skill set of the individual and the related activities needed to perform the functions.

Conclusion

The control procedures were suitably designed and existed at the time of our audit.

Personnel Controls: Security Issues

Control Objective

Appropriate consideration is given to security issues when management and staff are hired and terminated.

Control Procedures

1. Policies and procedures relating to all aspects of the hiring and termination of employees have been developed and implemented.
2. At the time of initial employment, all employees and contract personnel are required to acknowledge that they have read TES's Business Conduct Guidelines, and to sign an "Employee Agreement Respecting Confidential Information and Intellectual Property."
3. TES managers are responsible for ensuring that the security requirements for terminated employees are met.
4. TES senior management is involved in all involuntary terminations to ensure that the termination is immediate, and that all security requirements take place immediately.

Conclusion

The control procedures were suitably designed and existed at the time of our audit.

Security Policies and Procedures

Control Objective

Information technology security is operated in an efficient and effective manner.

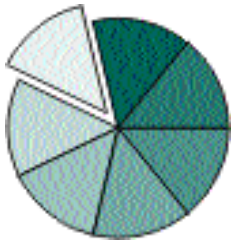
Control Procedures

1. Policies and procedures exist that support the efficient and effective implementation, operation and maintenance of security measures.
2. Policies, procedures and standards are communicated to the appropriate departments.

Conclusion

The control procedures were suitably designed and existed at the time of our audit.

G. Information Technology Back-up and Recovery



As organizations continue to become increasingly reliant upon information technology, there is an heightened importance of information technology back-up and the ability for recovery after an interruption. Information technology recovery planning has become an important part of business continuity planning, where the restoration of systems are prioritized according to their business need for availability.

Disaster Recovery Planning, Back-up and Recovery, and Insurance

Control Objective

Critical information systems processing functions can be resumed promptly in the event of significant disruption to normal computer operations.

Control Procedures

Disaster recovery planning:

1. A Disaster Recovery Plan exists for the recovery of the MVS processing platform in the event of service interruption.

2. The Disaster Recovery Plan:
   - considers yearly capacity planning,
   - includes details of team members and contact procedures, and
   - includes emergency evacuation procedures.
3. An agreement exists with SunGard for the use of alternate processing facilities for the MVS processing platform in the event of a disaster affecting the TES facilities.
4. Formal assignment of disaster-related responsibilities is included in the job descriptions of the MVS group, Storage Management group, Database Administration and Operation staff.
5. The plan describes each team's role and procedures during all phases of the recovery plan, including initiation, hotsite restoration, assessment, interim site migration and reconstruction (if necessary), and return to the home site.
6. Damage impact assessments are part of the Disaster Recovery Plan.
7. The Disaster Recovery Plan is tested on an annual basis. The most recent test was performed in July 2001.
5. Joint ITSD and TES meetings are held with the participating clients before and after the test to discuss the results and suggest new methods to help improve the process.
6. The test results are documented and appropriate action is taken to resolve any problems encountered.
7. The Disaster Recovery Plan is updated after every disaster recovery test.

Back-up and Recovery:

8. Back-up procedures exist for full image and incremental back-ups of system and user files and datasets and application databases.

9. Procedures exist for all normal operating activities and functions such as restart and recovery procedures.
10. Data, system and documentation back-ups are stored off-site and kept for specified periods.
11. Logical access to back-up tapes is secured by access control software.
12. Where appropriate, the back-up logs are reviewed and the existence and usability of the data back-ups are periodically verified.
13. Critical files, which would need to be recovered, are defined.

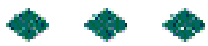
Insurance:

14. The Risk Management department at TELUS administers computer equipment insurance.
15. Business interruption insurance is covered under the above policy.
16. Boiler and machinery insurance is covered under the above policy.
17. All insurance coverage is reviewed and revised annually by the Audit Committee of the Board.

Conclusion

Mission critical programs, data files, computer resources and operating systems are covered by the Disaster Recovery Plan. Information technology support requirements for business processes deemed less critical are also addressed. If the computer center was damaged or inaccessible for an extended period of time, critical application processing would be re-established within 24 hours. All other non-development applications would be restored as time and resources permit, probably within 48 to 72 hours.

The control procedures were suitably designed and existed at the time of our audit.



Response from the Ministry of Management Services

The Ministry of Management Services is pleased to respond to the Auditor General's findings on internal control procedures in the MVS Environment.

Firstly, I would like to express my appreciation for the comprehensive analysis the auditing team has provided. The Ministry engaged the Auditor General because we believe audits such as this are important tools to ensure that we evolve to meet changes in technology and business requirements. Most of the environment management practices that were evaluated have been in place for over 20 years and they received an unqualified opinion in a similar audit performed in 1997.

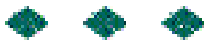
There have been no known security breaches in the MVS environment. However, the change from an in-house to outsourced delivery model and the increased use of the Internet have significantly impacted the security and control of this computing environment. These changing conditions demand a change in practices and this study will help us to meet that challenge.

Regarding the findings of the study, at the time of writing, most of the Auditor General's recommendations have been implemented. We have adjusted the access privileges of ministry and Telus Enterprise Solutions (TES) system staff to improve accountability and control over these functions. We have also adjusted any user accesses that were inconsistent with security policy and are implementing monitoring procedures to identify future violations quickly.

Projects are underway at the Ministry and TES to address the remaining recommendations, with planned completion by February 2003:

- more complex user authorization scheme for government applications that use the Information Management System (IMS) transaction processing monitor will be implemented, thereby allowing access to be granted and restricted on a more granular basis.
- Disaster recovery backup data will be assigned specifically to the data owner to reduce the risk of inappropriate access to data during a disaster recovery exercise.
- An additional layer of authentication will be implemented in the Customer Information Control Systems regions (CICS) to increase the security of these applications.

These changes have some potential to affect the government's applications, so we will be working closely with the application owners to ensure any service impacts are minimized.



Appendices

Appendix A

Summary Financial Statement Audit Methodology

When examining for the purpose of expressing an opinion on financial statements, auditors are expected to comply with established professional standards, referred to as generally accepted auditing standards. The principal source of these standards in Canada is the Canadian Institute of Chartered Accountants (CICA).

Generally accepted auditing standards consist of three main areas. There are general requirements that the auditor be properly qualified to conduct and report on an audit, and that he or she carry out the duties with an objective state of mind. Further standards outline the key technical elements to be observed in the conduct of an audit. Finally, reporting standards set out the essential framework of the auditor's report on the financial statements.

In addition to these broad standards, the CICA makes other, more detailed, recommendations related to matters of auditing practice.

Application of the Standards

We carry out extensive examinations of the accounts and records maintained by the ministries and central agencies of government, and by the Crown corporations and other public bodies of which the Auditor General is the auditor.

Also, with respect to Crown corporations that are audited by other auditors and that form part of the Summary Financial Statements, we obtain various information and assurances from those other auditors which enable us to rely on their work in conducting our audit of the government's accounts. This information is supplemented by periodic reviews by our staff of those auditors' working paper files and audit procedures.

Throughout these examinations, the Office of the Auditor General complies with all prescribed auditing standards in the conduct of its work. It must be realized, however, that the Auditor General's opinion on a set of financial statements does not guarantee the absolute accuracy of those statements. In auditing the government financial statements, or of any large organization, it is neither feasible nor economically desirable to examine every transaction. Instead, using our knowledge of the government's business, its methods of operation and systems of internal control,

we assess the risk of error occurring and then design audit procedures to provide reasonable assurance that any errors contained in the financial statements are not, in total, significant enough to mislead the reader as to the government's financial position or results of operations.

When determining the nature and extent of work required to provide such assurance, we consider two main factors: *materiality,* which is expressed in dollar terms, and *overall audit assurance,* expressed in percentage terms.

- *Materiality* relates to the aggregate dollar amount which, if in error, would affect the substance of the information reported in the financial statements, to the extent that a knowledgeable reader's judgement, based on the information contained in the statements, would be influenced.

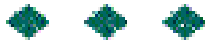
  In our audit of the Summary Financial Statements, we have assumed that an error in the current year's operating results in excess of one-half of 1% of the gross expense of the government would be considered material.

- *Overall audit assurance* represents, in percentage terms, how certain the auditor wants to be that the audit will discover errors, if any, in the financial statements, which in total exceed materiality.

  In our audit of the Summary Financial Statements, we planned our work so as to achieve an overall audit assurance of 95% that the audit would detect total error in excess of materiality. In choosing the level of assurance, we consider factors such as the expectations of the users of the financial statements and the nature of the audit evidence available.

In planning our audits of financial statements, we exercise professional judgment in determining the application of these two key factors. Professional judgment is influenced by our knowledge of the requirements of readers of the financial statements, and by what is generally accepted as being appropriate by auditors of similar organizations.

We continuously revise and update our auditing methodology to keep pace with auditing best practices.



Appendix B

Government Organizations Included in the 2001/2002 Summary Financial Statements, and Their Auditors

	Audited by	
	Auditor General	Private Sector Auditors
552513 British Columbia Ltd.	✓	
577315 British Columbia Ltd.	✓	
580440 B.C. Ltd.	✓	
632121 British Columbia Ltd.	✓	
634349 British Columbia Ltd.	✓	
B.C. Community Financial Services Corporation		✓
B.C. Festival of the Arts Society		✓
B.C. Games Society		✓
B.C. Health Care Risk Management Society		✓
B.C. Pavilion Corporation		✓
BC Society for the Distribution of Gaming Revenue to Charities	✓	
BC Transportation Financing Authority	✓	
BCIF Management Ltd.		✓
British Columbia Arts Council[1]		
British Columbia Assessment Authority	✓	
British Columbia Buildings Corporation		✓
British Columbia Enterprise Corporation	✓	
British Columbia Ferry Corporation		✓
British Columbia Health Research Foundation		✓
British Columbia Heritage Trust		✓
British Columbia Housing Management Commission		✓
British Columbia Hydro and Power Authority		✓
British Columbia Immigrant Investment Fund Ltd.		
British Columbia Liquor Distribution Branch[2]	✓	
British Columbia Lottery Corporation		✓
British Columbia Railway Company		✓
British Columbia Securities Commission	✓	

[1] The entity's financial statements were unaudited.
[2] A special operating agency under the Ministry of Competition, Science and Enterprise

Appendix B

	Audited by	
	Auditor General	Private Sector Auditors
British Columbia Trade Development Corporation		✓
British Columbia Transit		✓
Canadian Blood Services		✓
Columbia Basin Trust		✓
Columbia Power Corporation	✓	
Creston Valley Wildlife Management Authority Trust Fund	✓	
Discovery Enterprises Inc.		✓
Duke Point Development Limited	✓	
First Peoples' Heritage, Language and Cultural Council		✓
Fisheries Renewal BC	✓	
Forensic Psychiatric Services Commission		✓
Forest Renewal BC	✓	
New Forest Opportunities Ltd.	✓	
Homeowner Protection Office	✓	
Industry Training and Apprenticeship Commission	✓	
Insurance Corporation of British Columbia		✓
Land and Water British Columbia Inc.	✓	
Legal Services Society	✓	
Oil and Gas Commission	✓	
Okanagan Valley Tree Fruit Authority		✓
Organized Crime Agency of British Columbia Society		✓
Pacific National Exhibition		✓
Private Post-Secondary Education Commission		✓
Provincial Capital Commission	✓	
Provincial Rental Housing Corporation		✓
Rapid Transit Project 2000 Ltd.		✓
Science Council of British Columbia		✓
Tourism British Columbia	✓	
Vancouver Trade and Convention Centre Authority	✓	
Victoria Line Ltd.	✓	

Appendix C

The 2001/2002 Summary Financial Statements

Appendix D

Office of the Auditor General: 2002/03 Reports Issued to Date

Report 1

Building a Strong Work Environment in British Columbia's Public Service: A Key to Delivering Quality Service

Report 2

Follow-up of Performance Reports, June 2002

Report 3

A Review of Financial Management Issues in the Office of the Police Complaint Commissioner

Report 4

Monitoring the Government's Finances

Report 5

Managing Contaminated Sites on Provincial Lands

Report 6

Review of Estimates Related to Vancouver's Bid to Stage the 2010 Olympic Winter Games and Paralympics Winter Games

Report 7

Building Better Reports:
Our Review of the 2001/02 Reports of Government

Report 8

Follow-up of Performance Reports, January 2003

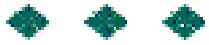
Report 9

A Review of Government Oversight of Multi-Employer Public Sector Pension Plans in British Columbia

Report 10

Adopting Best Practices in Government Financial Statements 2001/2002

These reports and others are available on our website at http://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 2003