Finance

8

8 Finance

Main points

The General Revenue Fund financial statements continue to account for pension costs and obligations to and from the Growth and Financial Security Fund inappropriately. Because of this inappropriate accounting, the statements report the net debt and annual surplus inaccurately. If the Government used proper accounting, net debt at March 31, 2010 would be $8.46 billion instead of the recorded net debt of $3.64 billion and the 2009-10 annual deficit would be $173 million instead of the recorded surplus of $425 million. Our audit report on the Fund's financial statements advises readers of these errors.

During 2009-10, Ministry of Finance (Finance) and three of its pension-related agencies made progress in completing their business continuity plans but further work remains. This work includes receiving confirmation from the Information Technology Office that it can meet Finance's disaster recovery and availability requirements. Also, Finance needs to make further improvements in its information technology processes such as following its procedures to remove unneeded user access to its information systems and data promptly.

Public Employees Benefits Agency (PEBA), a part of the Ministry that administers various government pension and benefit plans, needs to follow its policies for the timely review and approval of bank reconciliations and journal entries. It had adequate controls to secure its information technology (IT) systems and data except it needs to:

- periodically review and test the effectiveness of its IT security policies
- comply with its security policy of monitoring software developers' access to its information systems and data
- implement its disaster recovery plan
- implement its approved policies and procedures for making changes to its information technology infrastructure

This page left blank intentionally.

Introduction

This chapter sets out the results of our audit of the financial statements of the Government of Saskatchewan along with the results of our audits of the Ministry of Finance (Finance) and its agencies for the year ended March 31, 2010.

Also, it contains the results of our audit of the Public Employees Benefits Agency's (PEBA) central controls to protect its information technology systems and data, and an update of recommendations from our 2008 audit of PEBA's processes to manage service delivery. Finally, it includes the status of related recommendations of the Standing Committee on Public Accounts (PAC).

Background

Treasury Board is responsible for setting accounting policies and approving the Summary Financial Statements and the General Revenue Fund (GRF) financial statements prior to their publication in the Public Accounts – Volume 1. Finance is responsible for the preparation of these statements in accordance with accounting policies set by Treasury Board. In addition, Finance is responsible for setting and using effective controls to permit the preparation of these financial statements.

Finance helps the Government manage and account for public money. Its mandate is to provide options and advice to Treasury Board and Cabinet on managing and controlling the Government's finances. Its responsibilities include the following:

- administering and collecting provincial taxes
- arranging government financing, banking, investing, and borrowing
- administering certain public sector pension and benefit plans
- receiving revenues from taxation and transfers
- controlling spending from the General Revenue Fund (GRF)
- maintaining ministry-wide revenue and expense systems including the financial modules of the computerized Multi-informational Database Applications system (called MIDAS Financials)
- providing information, advice, and analysis on:

- government-wide fiscal and economic policies including tax policy alternatives and budgetary decisions relating to the GRF
- strategic policy development and analysis on matters related to public sector compensation and management or collective bargaining
- financial management and accounting
- annual performance planning, measuring, and reporting processes

Special purpose funds and agencies

Finance administers and is responsible for the following special purpose funds and agencies (agencies). Each of the agencies (except for the Growth and Financial Security Fund) provides the Legislative Assembly with audited financial statements; some agencies also provide an annual report.

Year ended March 31
General Revenue Fund
Growth and Financial Security Fund[1]
Judges of the Provincial Court Superannuation Plan
Public Employees Benefits Agency Revolving Fund
Public Employees Pension Plan
Public Service Superannuation Plan
Saskatchewan Pension Annuity Fund
Saskatchewan Watershed Authority Retirement Allowance Plan

Year ended December 31
Extended Health Care Plan
Extended Health Care Plan for Certain Other Employees
Extended Health Care Plan for Certain Other Retired Employees
Extended Health Care Plan for Retired Employees
Municipal Employees' Pension Commission
Municipal Financing Corporation of Saskatchewan
Public Employees Deferred Salary Leave Fund
Public Employees Dental Fund
Public Employees Disability Income Fund
Public Employees Group Life Insurance Fund
Saskatchewan Government Insurance Service Recognition Plan

[1] This Fund does not prepare financial statements and is not required to do so.

Saskatchewan Pension Plan
Saskatchewan Power Corporation Designated Employee Benefit Plan
Saskatchewan Power Corporation Pre-1996 Severance Plan
Saskatchewan Water Corporation Retirement Allowance Plan
SaskEnergy Retiring Allowance Plan
SaskPower Supplementary Superannuation Plan

Overview of the Ministry's finances

For the year ended March 31, 2010, Finance administered revenues of $8.0 billion and spent approximately $0.8 billion. Major revenues include:

	Original Estimates	Actual
	(millions of dollars)	
Taxes	$ 4,450.9	$ 4,723.9
Transfers from the Federal Government	1,188.7	1,164.2
Transfers from government entities	760.7	1,209.9
Non-renewable resources	461.8	475.6
Other own-source revenue	328.9	401.5
Total	$ 7,191.0	$ 7,975.1

The following is a list of major programs and spending:

	Original Estimates	Actual
	(millions of dollars)	
Revenue	$ 20.0	$ 19.7
Research and development tax credit	18.0	18.0
Provincial comptroller	9.4	8.4
Central management and services	7.5	6.2
Budget analysis	5.3	4.9
Treasury and debt management	2.9	2.6
Personnel policy secretariat	0.8	0.6
Amortization of capital assets[2]	1.0	0.9
Other	0.1	0.1
	65.0	61.4
Finance – servicing government debt	502.5	480.0
Public service pension and benefits[3]	264.4	278.2
Total spending	$ 831.9	$ 819.6

[2] Amounts do not include capital asset acquisitions of $280,000 (original estimate) and $38,000 (actual).
[3] Finance determines the estimates for public service pension and benefits using the cash basis of accounting instead of the accrual basis. Using the accrual basis of accounting, the actual expense is $278.2 million-restated from $265.2 million (the cash-based amount reported in Finance's annual report) to include $13.0 million of unrecorded pension costs.

Finance's annual report sets out differences between actual and budgeted revenues and expenses and explains significant differences.

Audit conclusions and findings

To form our opinion on the Public Employees Pension Plan, our Office worked with Meyers Norris Penny LLP, the Plan's appointed auditor. We used the framework recommended by the *Report of the Task Force on Roles, Responsibilities and Duties of Auditors.*[4]

In our opinion for the year ended March 31, 2010:

- **the Government's Summary Financial Statements included in the Public Accounts 2009-10 Volume 1 are reliable**
- **the General Revenue Fund's financial statements included in the Public Accounts 2009-10 Volume 1 are reliable except for not recording all amounts owed for pension liabilities and improper recording of transfers between the General Revenue Fund and the Growth and Financial Security Fund**
- **the financial statements of the other above-listed agencies with a March year-end are reliable**
- **Finance and its agencies with a March year-end had adequate rules and procedures to safeguard public resources except for matters reported in this chapter**
- **Finance and its agencies with a March year-end complied with authorities governing their activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing except for matters reported in this chapter**

The law requires us to report when a special warrant approved the payment of public money. For the year ended March 31, 2010, the Government approved, through Orders in Council, spending of

[4] This report is available on our website at www.auditor.sk.ca/rrd.html.

$134.3 million; the Legislative Assembly later approved these amounts through an appropriation act.

Payroll service agreement needed

Finance does not maintain a current service level agreement (SLA) with Public Service Commission (PSC) that clearly assigns responsibilities for key payroll activities.

PSC provides payroll services to Finance. Finance spends about $23.6 million each year on salaries and benefits.

Finance's SLA with PSC that set out the responsibilities of each party for key payroll activities expired on March 31, 2009. At August 2010, Finance had not extended or renewed its SLA with PSC.

Lack of a current, signed service agreement increases the risk that Finance may not receive the payroll services it needs.

1. **We recommend that the Ministry of Finance maintain a current service level agreement with the Public Service Commission for the provision of payroll services.**

Better information technology processes needed

Finance needs to improve its information technology (IT) processes in the following areas:

- reach agreement with the Information Technology Office (ITO) over IT disaster recovery to meet Finance's requirements
- require reporting from ITO on its adequacy of its security and availability of Finance's computer systems and data
- follow its processes for removing users' access to its computer systems promptly

Since September 2005, Finance has used ITO to provide certain IT services. Finance remains responsible to have adequate policies to support its IT requirements.

Finance's service level agreement (SLA) with ITO sets out the scope, level, and quality of services ITO provides. However, the current SLA does not include adequate provisions for the on-going availability of Finance's key information technology services or disaster recovery processes, expectations, and reporting requirements.

In 2009-10, Finance finalized its business continuity plan (BCP).[5] Finance advised ITO of its disaster recovery and availability requirements. Finance did not receive confirmation from ITO that ITO can provide disaster recovery and availability that would meet the requirements set out in Finance's BCP.

Since our 2006 Report – Volume 3, we have recommended that the Ministry of Finance confirm, in writing, processes ITO uses to address specific IT security and disaster recovery requirements. In March 2007, PAC agreed with our recommendation. We continue to make this recommendation.

In 2009-10, Finance received limited information from ITO about the adequacy of ITO's controls for keeping Finance's computer systems and data secure and available. During 2009-10, Finance received some information verbally. Finance has not formally required ITO to provide this information (e.g., through its SLA with ITO).

Finance relies on its computer systems and data to deliver its programs. Finance needs to know of ITO's control weaknesses[6] (if any) so that it can assess the impact on its computer systems and data and take the necessary steps to mitigate the impact.

2. We recommend that the Ministry of Finance require the Information Technology Office (ITO) to give it, each year, information on the adequacy of ITO's controls for keeping Finance's computer systems and data secure and available.

During 2009-10, Finance did not follow its processes for removing users' access to its computer systems on a timely basis. Finance has adequate processes for removing user access from individuals who no longer work

[5] **Business Continuity Plan** - A plan by an organization to respond to unforeseen incidents, accidents, and disasters that could affect the normal operations of the organization's critical operations or functions.
[6] Provincial Auditor Saskatchewan 2009 Report – Volume 3 (Chapter 12).

for the Ministry or who have changed roles and do not require such access.

During our audit, we noted ten instances where access was not removed promptly. Finance was not aware of these instances until our audit brought them to its attention. If unneeded access is not removed promptly, it increases the risk of inappropriate access and unauthorized changes to the Finance's systems and data.

3. We recommend that the Ministry of Finance follow its processes for removing unneeded user access to its information technology systems and data promptly.

Implementation of past recommendations needed

In our previous reports, we made recommendations relating to Finance's treasury management. As noted in Exhibit 1, these recommendations remain outstanding. We continue to make the recommendations contained in Exhibit 1.

Exhibit 1 – Summary of previous outstanding recommendations

RECOMMENDATION (INITIAL REPORT)	STATUS PAC	ACTIONS FINANCE TOOK IN 2009-10	STATUS OF RECOMMENDATION
Treasury management			
We recommend that the Ministry of Finance set out its investment expectations in sufficient detail to make possible the measurement and evaluation of its investment performance. (2009 Report – Volume 1 - Chapter 5)	PAC agreed with these recommendations on September 1, 2009.	Finance researched and considered potential benchmarks for measuring performance. It developed a quarterly report which will communicate more extensive information regarding investment expectations and results to senior management. It expects to provide this report to the Minister and Deputy Minister of Finance starting in 2010-11.	Partially implemented.

RECOMMENDATION (INITIAL REPORT)	STATUS PAC	ACTIONS FINANCE TOOK IN 2009-10	STATUS OF RECOMMENDATION
We recommend the Ministry of Finance monitor and report publicly on the performance of the investments in its sinking funds. (2009 Report – Volume 1 - Chapter 5)		Finance is researching relevant basis for reporting the performance of the sinking funds publicly.	Not implemented.
We recommend the Ministry of Finance document its key treasury management procedures in sufficient detail so it can continue to operate effectively after staff turnover. (2009 Report – Volume 1 - Chapter 5)		Finance developed a manual to assist with the processing of wire payments, identified opportunities to further improve documentation, and made plans to complete the following in 2010-11: ♦ implement a debt system to centralize information associated with debt issues ♦ document procedures relating to Saskatchewan Savings Bonds Finance's other key documentation of its investing and borrowing procedures includes: ♦ a manual that documents the money market investing and short-term debt issuance procedures ♦ a checklist of procedures for issuance of long-term debt	Partially implemented.

General Revenue Fund

Background

The General Revenue Fund (GRF) is a special purpose fund established under *The Financial Administration Act, 1993*. By law, the Government must deposit into the GRF all public money other than those over which the Legislative Assembly has no power of appropriation and those otherwise specifically disposed of by the Legislative Assembly (e.g., revenues of Crown corporations, agencies, other special purpose funds, and revolving funds). The Government must pay out of the GRF

expenses and any loans, advances, or investments as permitted or required by a vote of the Legislative Assembly.

Continued use of inappropriate accounting policies

Treasury Board does not use Canadian generally accepted accounting principles for the public sector (GAAP) to account for pension and disability (pension) costs or to record transfers to and from the Growth and Financial Security Fund when preparing the GRF financial statements.

It is important that governments use GAAP to prepare their financial statements. Use of GAAP helps ensure the financial results are presented fairly and free from bias. It is not appropriate for governments to set accounting policies based on their own preferences.

Financial statements should reflect the costs of decisions made during the year. In addition, as the Government uses the GRF's annual surplus as one of its key performance indicators, users should consider the impact of the errors in the GRF financial statements.

Because the Government uses inappropriate accounting policies, the GRF financial statements report net debt and annual surplus inaccurately. If the Government had accounted for all transactions properly, the statements would have recorded net debt of $8.46 billion instead of $3.64 billion at March 31, 2010 and recorded a deficit of $173 million instead of a surplus of $425 million for the year ended March 31, 2010.

Exhibit 2 below sets out, by line item of the affected statement within the GRF financial statements, the amount reported in that statement, the amount that should have been reported in that statement, the difference between these two amounts, and the reason for that difference.

Exhibit 2

Line item on financial statements	Amount reported in statements	Amount that should be reported in statements	Difference Amount reported is: Overstated (too high) Understated (too low)	Reason for difference
Statement of Financial Position				
Total Financial Assets	$3.69 billion	$4.65 billion	$958 million (understated)	Unrecorded "Due from Growth and Financial Security Fund"
Total Liabilities	$7.33 billion	$13.11 billion	$5.78 billion (understated)	Unrecorded pension and a disability plan debt
Net Debt	$3.64 billion	$ 8.46 billion	$4.82 billion (understated)	Net impact of not recording the above amounts
Accumulated Deficit	$546 million	$5.37 billion	$4.82 billion (understated)	Net impact of not recording the above amounts
Statement of Operations				
Total Expense	$10.10 billion	$10.44 billion	$341 million (understated)	Unrecorded pension and a disability plan costs for current year
Transfer to/from the Growth and Financial Security Fund	$257 million	$ ---	$257 million (overstated)	Inappropriately including net transfer as a revenue
Surplus	$425 million	($173 million)	$598 million (overstated)	Net impact of above errors on current year surplus

Because the errors significantly impair the usefulness of these financial statements, we have qualified our auditor's report on the GRF financial statements published in *Public Accounts 2009-10 Volume 1*. "Qualified" audit reports are not normal and should cause concern for legislators and the public. Our audit report advises readers of the errors in the financial statements.

We continue to recommend that the General Revenue Fund's financial statements record pension costs and transfers in accordance with Canadian generally accepted accounting principles for the public sector. In February 2002, PAC disagreed with our recommendation.

Public Employees Benefits Agency and pension plans it administers

Background

The Public Employees Benefits Agency (PEBA) is part of the Ministry of Finance. PEBA administers government pension and benefit plans. This includes the Public Employees Pension Plan (PEPP) and Public Service Superannuation Plan (PSSP). PEBA serves about 79,000 active and inactive (deferred) members, pensioners, and surviving spouses and dependents of these plans.[7]

PEBA recovers its costs to administer the pension and benefit plans by charging the plans based on the costs incurred for each plan. At March 31, 2010, the total assets of these pension and benefit plans are approximately $6.1 billion.

For the year ended March 31, 2010, PEBA incurred $12.6 million in administration costs and recovered those costs from the plans. At March 31, 2010, PEBA held assets of $5.9 million. PEBA's *2009-10 Annual Report* includes the PEBA Revolving Fund's audited financial statements.

The Public Employees Pension Board is responsible for *The Public Employees Pension Plan Act*. The Board manages PEPP, a defined contribution pension plan. Its primary objective is to provide retirement benefits to PEPP members in accordance with the law.

PEPP's *2009-10 Annual Report* included its audited financial statements. These financial statements report contributions of $103 million from employees and $115 million from employers, investment income of $150 million, and an increase in market value of the investments of $585 million. For the year, PEPP incurred administrative expenses of $15 million and made transfers or payments out of PEPP of $112 million. At March 31, 2010, PEPP held assets of $4.4 billion.

The Public Superannuation Board is responsible for the administration of *The Public Service Superannuation Act* and other relevant legislation. The Board manages PSSP, a defined benefit pension plan. PSSP consists of the Public Service Superannuation Fund, the Anti-

[7] Ministry of Finance. (2010). *2009-10 Annual Report*. Regina: Author p. 40.

Tuberculosis League Employees Superannuation Fund, and the Saskatchewan Transportation Company Employees Superannuation Fund. The Board's primary objective is to provide superannuation allowances to employees who retire and to the dependents of deceased superannuates and employees, in accordance with governing legislation.

In 2009-10, PSSP received contributions of $2 million from employees and $115 million from the General Revenue Fund. At March 31, 2010, the PSSP held assets of $9 million and had liabilities of $1,927 million.

Business continuity plans needed

In our 2009 Report – Volume 3 and past reports, we recommended that PEBA complete a business continuity plan for the pension and benefit plans it administers. In our 2009 Report – Volume 3 and past reports, we made a similar recommendation for the PSSB and PEPP, respectively. PAC agreed with our recommendations. We continue to make these recommendations.

The critical services that PEBA and these Plans provide include receiving and recording contributions from employers and employees, handling transfers, and providing termination benefits, death benefits, and retirement benefits to members. PEBA and each of these plans must be able to provide these services even if a disaster disrupts its operations and services. Without an adequate business continuity plan, they may not be able to provide their critical services.

Exhibit 3 below sets out the actions that PEBA and each Plan took in 2009-10 towards completing their business continuity plans.

Exhibit 3

Agency	Actions taken in 2009-10
PEBA	PEBA continued to work on a business continuity plan for its critical services. It had developed a plan, but not tested it. Until PEBA tests its plan, there is a risk that the plan will not meet its business continuity needs.
PEPP	PEPP completed developing a business continuity plan for its critical services. PEPP needs to test the effectiveness of the business continuity plan. Management told us it expects to test its business continuity plan next year.
PSSB	The Board continued to work on completing a business continuity plan for its critical services. It had developed a plan, but not tested it. Until the Board tests its plan, there is a risk that the plan will not meet its business continuity needs.

Need to follow policies for bank reconciliations and journal entries

PEBA has written policies and procedures for preparing, independent reviewing, and approving bank reconciliations and journal entries. Its policies and procedures specify that all reviews and approvals must be completed within 45 days of month end.

Timely reconciliation of recorded bank balances to bank records provides a check that all charges to the bank accounts are proper, and all money received is deposited promptly and to the right bank account. Timely preparation of journal entries ensures that all accounting records are updated and accurately maintained. Review of bank reconciliations and journal entries independent of preparation helps to ensure the work is properly done when expected.

We found that over half of the time, PEBA did not comply with its policies and procedures for reviewing and approving PSSP bank reconciliations and journal entries. For example, PEBA did not perform the independent review and approval of the PSSP December 2009 bank reconciliation and journal entries until March 22, 2010. Also, in other instances there was no evidence of independent review and approval of bank reconciliations and journal entries.

Without following the policies governing the review and approval of bank reconciliations and journal entries, there is increased risk that PEBA may not promptly detect errors and losses in the PSSP's bank balances and accounting records.

4. We recommend that the Public Employees Benefits Agency follow its policies for the timely review and approval of bank reconciliations and journal entries for the Public Service Superannuation Plan.

Retired PSSP members' pensions

Since our 2001 Spring Report, we have recommended that the Public Service Superannuation Board establish rules and procedures to ensure that all retired members who are receiving a pension and who return to work for the Government are paid in accordance with *The*

Superannuation (Supplementary Provisions) Act (Act). Alternatively, the Board should seek changes to the Act. In November 2001, PAC agreed with our recommendation. We continue to make this recommendation.

The Board of PSSP needs information about retired PSSP members who are receiving a pension and have returned to work for the Government. The Board needs this information to ensure it pays pensions in accordance with the law.

Requirements for stopping the pensions of retired PSSP members who return to work for the Government are set out in section 27 of the Act. The Act allows retired members to work as temporary, casual, or provisional employees for up to six months in a fiscal year without a reduction in their pensions. The Act requires the PSSP Board to stop the pension of a retired member who works for the Government for more than six months in a fiscal year. The Act also requires the PSSB Board to stop the pension of a retired member that the Government re-hires as a permanent employee when that member starts work.

However, the PSSP Board does not have rules and procedures to know if retired members are working for the Government. It relies on retired PSSP members notifying it upon re-employment with the Government. As a result, the PSSP Board cannot ensure that all pensions it paid comply with the law. Accordingly, we cannot determine if the PSSP Board complied with section 27 of the Act.

Legislative requirements for annual reports are inconsistent – PSSP

In our 2009 Report – Volume 3, we recommended that the Public Service Superannuation Board seek changes to its legislation to remove personal information disclosures required in its annual report by section 69(1) of *The Public Service Superannuation Act*. We continue to make this recommendation.

To be a good accountability document, an annual report should describe the Board's goals, objectives, how it manages its key risks, what it has done, where it is now, and what it plans to do. This information helps stakeholders assess the performance of an organization.

Section 69(1) of *The Public Service Superannuation Act*, requires the PSSP Board to submit an annual report to the minister showing the following:

- all the names of member employees who have retired, who have died during the last preceding fiscal year
- the position and government agency they worked for
- the amount of salary payable and age at retirement or death
- the cause of early retirement
- the amount of superannuation allowances granted to each employee

Generally, pension plans do not provide this type of detailed information about their members in their annual report. This type of detailed and personal information disclosure does not provide useful information to help make the annual report a good public accountability document.

In recent years, for some pension plans, legislative requirements to require disclosure of detailed personal information were removed. We are not aware of the reason for different legislative requirements for the disclosure of information in the PSSP annual report as compared to other Saskatchewan public sector pension plans. The detailed personal disclosure requirements do not help users assess PSSP's actual performance against its planned goals and objectives and are inconsistent with legislative requirements and annual report disclosures of other government pension plans.

Processes to manage service delivery—a follow-up

Background

PEBA has signed service agreements with its major plans including PEPP and MEPP. It must provide its services in accordance with the requirements and targets described in the service agreements. Rigorous service delivery processes at PEBA help promote a clear understanding of roles and responsibilities and maintain effective relationships with the plans.

Managing service delivery—a follow-up

In our 2008 Report – Volume 1, Chapter 5 (p. 67) we concluded that PEBA had adequate processes to manage the delivery of agreed-upon services to the pension and benefit plans except that it needed to explain significant differences between expected and actual results for each specific service standard described in the service agreements. We recommended that PEBA explain significant differences between expected and actual results for each specific service standard described in the service agreements. On August 28, 2008, PAC agreed with our recommendation.

As of August 31, 2010, we determined that PEBA has met our recommendation. PEBA includes explanations in quarterly reports to clients for specific service standards that do not meet expected targets as described in the service agreements.

Information technology security audit

Background

To carry out its responsibilities, PEBA must manage a wide range of pension and benefit information. PEBA uses information technology (IT) systems to manage this information and to provide pension and benefit information to its members. Securing pension and benefit information (ensuring its confidentiality, integrity, and availability) is vital to fulfilling PEBA's objectives including delivering its services and protecting the interests of its members.

Inadequate security could result in loss, inappropriate modification, and unauthorized disclosure of pension and benefit information. Unauthorized changes to the systems and data could compromise the integrity of the pension and benefit plans. Unauthorized disclosure of members' personal information (e.g., name, date of birth, social insurance number) could lead to the theft of their identity for fraudulent purposes.

Audit objective and conclusion

The objective of this audit was to assess whether PEBA had adequate controls to secure (i.e., protect the confidentiality, integrity, and availability

of) its information technology systems and data for the period October 1, 2009 to March 31, 2010.

Throughout our audit, we followed the *Standards for Assurance Engagements* published in the *CICA Handbook – Assurance*.

To conduct this audit, we used criteria to assess PEBA's processes. The criteria are based on the *Trust Services Principles, Criteria, and Illustrations* authored by the Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants and on international standards, literature, and reports of other legislative auditors. PEBA's management agreed with the criteria.

The criteria set out in the Exhibit 4 describe the key processes that we expected PEBA to use to secure its systems and data.

Exhibit 4–Audit criteria

To secure (i.e., protect the confidentiality, integrity, and availability of) its information technology systems and data, we expected PEBA would:

1. **Show management commitment to security**
   - Responsibility for security is clearly defined
   - IT planning supports security
   - Management has approved security policies and procedures
   - Management monitors security
2. **Protect systems and data from unauthorized access**
   - User access controls protect the systems and data from unauthorized access
   - Physical security controls protect against unauthorized access
3. **Keep systems and data available for operation**
   - System and data backups occur and are tested
   - Disaster recovery plans are in place and are tested
4. **Maintain the integrity of systems and data**
   - Change management processes exist and are followed
   - Computer operation processes exist and are followed

We conclude that the Public Employees Benefits Agency had adequate controls to secure (i.e., protect the confidentiality, integrity, and availability of) its information systems and data for the period October 1, 2009 to March 31, 2010 except it needs to:

- **periodically review and test the effectiveness of its IT security policies**
- **comply with its security policy of monitoring software developers' access to its information systems and data**
- **implement its disaster recovery plan**
- **implement its approved policies and procedures for making changes to its information technology infrastructure**

Key findings (by criterion) and recommendations

We describe below what we expected (in italics) and our key findings for each criterion together with our recommendations.

Show management commitment to security

Management commitment includes clearly defining security responsibilities and segregating incompatible functions. We expected PEBA would have a member of senior management who leads an information technology division. We also expected PEBA would plan, implement, and monitor compliance with security policies and procedures.

PEBA clearly defines responsibility for security through its organizational structure and written job descriptions. PEBA also prepares an IT strategic plan that complements its strategic plan. In addition, PEBA has approved a number of IT security policies. New employees receive training on the security policies as part of their orientation process. These policies are readily available to staff.

PEBA does not periodically review the effectiveness of its security policies. For example, an annual review of security policies or a review when there are major changes to IT infrastructure or changes in technology helps keep security policies current and complete.

In 2009, PEBA implemented a system for certain pension members to access their pension information via the Internet and initiate changes to their plans. These pension members use unique user names and passwords for this purpose. PEBA does not have a procedure to address

the steps that it should take when these accounts become inactive (i.e., have not been used for a long time). Inactive accounts increase the risk of unauthorized access to members' personal information.

PEBA's policies do not require employees to annually acknowledge their awareness of PEBA's security policies and their compliance with them. An annual sign-off of awareness and compliance with security policies is an effective security awareness practice.

5. We recommend that the Public Employees Benefits Agency periodically review the completeness of its information technology policies.

PEBA does not periodically test the effectiveness of its IT security. The periodic testing of security using external experts helps management to monitor the adequacy of security. Independent vulnerability assessments and penetration testing can be effective for strengthening security.

6. We recommend that the Public Employees Benefits Agency periodically test the effectiveness of its information technology security.

Protect systems and data from unauthorized access

We expected PEBA to have adequate physical access and user access controls to protect its systems and data from unauthorized access.

Good physical access controls protect IT infrastructure from harm. Physical access controls protect computers and network devices from unauthorized access. For example, a locked door helps prevent unauthorized users from entering a server room.

User access controls ensure only approved people or processes can use an IT system. A common example of a user access control is a username and a password. The username identifies the user and the password grants access.

Protecting systems from unauthorized access is more critical with the increased use of the Internet and automated processes. PEBA needs to protect its data by configuring, updating, and monitoring its systems

against security threats. In addition, it needs to monitor service providers working on their systems.

PEBA's security policies adequately govern access to its systems and data. These policies require usernames with robust passwords, the authorization and periodic review of all access and the prompt removal of access for terminated employees. The policies also state that passwords should not be shared. This latter requirement is necessary for holding users accountable for the systems and data they access and change. PEBA complies with its policies.

PEBA's security policies adequately govern the access of external software developers (vendors) to its systems and data. Its policies discourage external access by vendors. Each request is to be evaluated on a risk versus benefits basis and access to applications is strictly monitored. Only one vendor has access to a pension plan application and its data but the remote access is ongoing and not monitored by PEBA. As a result, PEBA's confidential data is at increased risk of unauthorized disclosure. PEBA should comply with its policies governing external access by vendors.

PEBA has implemented security infrastructure and software (e.g., firewalls, intrusion detection systems, anti-virus software) to protect its systems and data from unauthorized access. PEBA keeps this infrastructure up to date. It also has implemented adequate physical access controls to protect its data centre.

7. We recommend that the Public Employees Benefits Agency comply with its security policy of monitoring software developers' access to its information systems and data.

Keep systems and data available for operation

We expected PEBA to have adequate processes to ensure its systems and data are available for operation when needed.

Even with good backup and recovery procedures, PEBA may not be able to continue its operations if a major problem occurred. Therefore, it should have a contingency plan to recover operations in the event of a disaster like a fire or tornado. Its systems should also have sufficient

capacity so non-catastrophic events like power outages will not cause applications to quit abruptly with the possibility of data loss.

PEBA has adequate processes for backing up its systems and data. For example, it does timely backups and stores its weekly backups off-site. It can restore specific data when requested. However, it does not always store an updated copy of master passwords for its systems off-site. This oversight could prevent PEBA from restoring its systems and data from the backups in the event of a disaster.

PEBA's IT infrastructure has the capacity to handle many non-catastrophic events. For example, it has a backup power supply (i.e., batteries and generator) to automatically provide power to keep systems running. PEBA depends on its e-mail system to promptly notify IT staff of data centre problems requiring immediate attention. It does not have a back-up monitoring and notification system in the event its e-mail system stops working. When emergencies are not promptly addressed, more serious problems may occur.

PEBA is highly reliant on its information systems to support its business and financial operations. PEBA has identified the need for a disaster recovery plan and business continuity plan. It has developed these plans. The plans are not yet implemented and tested. The lack of an implemented and tested disaster recovery plan increases the risk that PEBA could not restore systems and data in the event of a disaster. We have previously made similar recommendations.[8]

8. We recommend that the Public Employees Benefits Agency implement and test its disaster recovery plan.

Maintain the integrity of systems and data

We expected PEBA to have processes for maintaining the integrity of its systems and data by implementing adequate configuration, update, monitoring, and IT operation processes. Adequate processes require approving and testing system changes before implementation. PEBA

[8] See business continuity plan recommendations under heading "Public Employees Benefits Agency and pension plans it administers – Business continuity plans needed" and disaster recovery plan recommendation in Exhibit 5.

must also ensure that it has adequate processes for running and maintaining its computers.

Good change management processes help PEBA reduce unintended consequences arising from changes. Change management processes also provide management with the necessary documentation to control and monitor changes.

PEBA follows approved policies and procedures for making changes to its pension and benefit application programs. A quality assurance group, independent of those developing the changes, tests the changes before they are implemented. PEBA, however, has not implemented its approved policies and procedures for making changes to its IT infrastructure.

We describe other findings related to maintaining the integrity of systems and data (e.g., firewalls, virus protection software, etc.) earlier under the heading "Protect systems and data from unauthorized access."

9. We recommend that the Public Employees Benefits Agency implement its approved policies and procedures for making changes to its information technology infrastructure.

Glossary

Account—A unique identity set up on a computer or network that allows access to specific systems and data.

Anti-virus software—A program designed to identify and manage (block, segregate, or destroy) malicious software.

Application—A software program. This includes programs such as word processors, spreadsheets, database programs, accounting programs, etc.

Backup (noun)—A copy of systems or data to be used when the originals are not available (e.g., because of loss or damage).

Change management—An organized approach for introducing changes into a program or process, used to minimize unintended consequences.

Data centre—A central location for computer network hardware and software, especially storage devices for data.

Disaster recovery plan—A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

Firewall—A piece of hardware or software intended to restrict or block access to a network or computer. Firewalls can be set up to only allow certain types of data through.

IT infrastructure—An organization's computer and network assets.

Intrusion detection system (IDS)—Software and/or hardware designed to detect a security breach by identifying inappropriate access or changes taking place within a computer or network.

Network—A group of computers that communicate with each other.

Penetration test—Evaluating the security of a computer system or network by simulating an attack from a malicious source.

Server—A computer that hosts systems or data for use by other computers on a network.

User access controls—The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.

Vulnerability assessment—The process of identifying, evaluating, and prioritizing vulnerabilities (or weaknesses) in a system.

Status of other outstanding recommendations of the Standing Committee on Public Accounts

Exhibit 5 provides an update on recommendations previously made by PAC that are not yet implemented and are not discussed earlier in this chapter.[9]

Exhibit 5

PAC REPORT YEAR[10]	OUTSTANDING RECOMMENDATION	STATUS
Ministry of Finance (Pension Plans)		
2007	PAC concurs: 5-4 that the Public Employees Pension Plan should document its risk assessments and action plans to reduce the risks to an acceptable level for the computerized pension administration system.	**Not implemented** (as at March 31, 2010).
2007	PAC concurs: 5-2 that the Public Employees Pension Plan should prepare, approve and test a complete disaster recovery plan.	**Partially implemented** (as at March 31, 2010).
2009	PAC concurs: 4-4 that the Municipal Employees' Pension Commission have a written, tested, and approved disaster recovery plan.	**Partially implemented** (as at December 31, 2009).
Ministry of Finance		
2005	PAC concurs: 9-2 that the Government should direct all Treasury Board agencies to use an accountability framework that focuses on results.	**Partially implemented** (as at September 30, 2009). We expect to follow-up this recommendation in 2013.

[9] For the definitions of the key terms used in the exhibit, see Chapter 24 – Standing Committee on Public Accounts.
[10] PAC Report Year refers to the year that PAC first made the recommendation in its report to the Legislative Assembly.

PAC REPORT YEAR[10]	OUTSTANDING RECOMMENDATION	STATUS
2005	PAC concurs: 9-3 that the Government should require departments and Treasury Board agencies to publish their planned targets for major long-term results.	**Partially implemented** (as at September 30, 2009). We expect to follow-up this recommendation in 2013.
2009	PAC concurs: 9-4 that the Ministry of Finance set the desired outcomes of the provincial sales tax audit selection process in measureable terms.	**Partially implemented** (as at August 31, 2009). We expect to follow-up this recommendation in 2012.
2009	PAC concurs: 9-5 that the Ministry of Finance analyze the risks that businesses are not complying with provincial sales tax laws and rank identified risks according to their potential significance.	**Partially implemented** (as at August 31, 2009). We expect to follow-up this recommendation in 2012.
2009	PAC concurs: 9-6 that the Ministry of Finance document its audit strategy to address identified risks that businesses are not complying with provincial sales tax laws.	**Partially implemented** (as at August 31, 2009). We expect to follow-up this recommendation in 2012.
2009	PAC concurs: 9-7 that the Ministry of Finance direct its audit efforts based on an overall risk analysis of businesses not complying with provincial sales tax laws.	**Partially implemented** (as at August 31, 2009). We expect to follow-up this recommendation in 2012.
2009	PAC concurs: 9-8 that the Ministry of Finance require its senior management to receive reports on the effectiveness of the provincial sales tax audit selection process.	**Partially implemented** (as at August 31, 2009). We expect to follow-up this recommendation in 2012.

This page left blank intentionally.