Public Service Commission

20

Main points

PSC is a central human resource agency primarily for staff employed by government departments.

PSC is responsible for the computerized human resource administration and payroll system. This system contains the personnel and payroll information. PSC had adequate controls to protect the confidentiality, integrity, and availability of this system with two exceptions. First, it did not have adequate policies and procedures for: monitoring access of staff who use this system, documenting and testing changes made to the system, and providing departments with sufficient information to help them monitor their payroll. Second, although PSC had an approved disaster recovery plan to restore the system in event of a disaster, it had not tested the plan to make certain it works properly.

As a central agency for human resources management, PSC must lead human resources planning within government departments. We found PSC had addressed the two recommendations we made in our 2005 report. It adequately communicates to departments a manageable number of human resource priorities and uses a risk management framework to help identify and analyze of human resource risks.

Finally, we note PSC must complete its own human resource plan and enter into an agreement with the Information Technology Office (ITO) for information technology services it receives from ITO. A complete human resource plan will help it have the right staff at the right time. An agreement with ITO is essential so that PSC can monitor the services ITO provides.

Introduction

This chapter sets out a background of the Public Service Commission (PSC), the results of our audits of PSC, and actions taken on recommendations related to PSC's processes to lead human resource planning.

Background

Under *The Public Service Act, 1998*, PSC provides leadership and policy direction for the human resource management of staff employed primarily by government departments. Government departments employ about 11,000 permanent staff and about 1,000 seasonal staff.

PSC provides the human resource policy framework in which government departments must operate. It is also the employer representative for all the departments in labour negotiations. The quality and strength of PSC's policies and corresponding human resource strategies are important to not only the success of PSC but to the success of the departments.

PSC is also responsible for the new computerized human resource administration and payroll system called the Multi-informational Database Applications human resources and payroll module (MIDAS HR/Payroll) that began operating March 14, 2006. At March 31, 2007, nine departments used MIDAS HR/Payroll to manage employee information (e.g., benefits, salary, job assignment, and training) and process payroll transactions for 21 government agencies (primarily departments).

For further details on PSC's mandate and governing legislation, consult its publications at its website www.gov.sk.ca/psc.

Financial overview

The following are PSC's major programs and spending. For further detail, see PSC's 2006-2007 Annual Report available on its website.

	Original Estimates	Actual
	(in thousands of dollars)	
Central management and services	$ 2,150	$ 2,028
Human resource information services	5,890	6,411
Employee relations	1,837	2,020
Aboriginal career connections program	507	624
Human resource client service	3,779	4,385
Capital asset amortization	1,310	1,240
	$ 15,473	$ 16,708

Audit conclusions and findings

In our opinion, for the year ended March 31, 2007:

- **PSC had adequate rules and procedures to safeguard public resources and comply with authorities governing its activities except for the matters reported in this chapter**

- **PSC complied with authorities governing its activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing and investing except for the matter relating to employees' pay**

Better control over employees' pay needed

PSC needs to better control employees' pay.

During the year, PSC reviewed its payroll costs during its review of monthly financial reports. However, PSC did not adequately review the accuracy of key payroll data for each pay period prior to paying employees. As a result, employees' pay has not been approved in accordance with *The Financial Administration Act, 1993.*

This weakness increases the risk that employees may be paid incorrect amounts.

1. We recommend that the Public Service Commission adequately review the payroll for accuracy prior to paying its

employees to ensure that all employees' pay is approved in accordance with *The Financial Administration Act, 1993*.

Human resource plan needs improvement

In chapter 7 of our 2006 Report – Volume 3, we reported that PSC needed to improve its human resource plan. At March 31, 2007, PSC employed about 142 staff (based on full-time equivalents). Due to its February 2006 reorganization within the PSC, it did not change or update its human resource plan prior to the start of the 2007-08 fiscal year. At August 31, 2007, PSC had developed a revised plan that was not yet approved. We will assess this plan, if approved, in our next audit.

We continue to recommend that Public Service Commission revise its departmental human resource plan to include the following:

- a prioritized listing of human resource risks specific to PSC
- detailed strategies to bridge identified gaps in human resource needs specific to PSC
- assignments of responsibility and deadlines for implementing major strategies[1]

The Standing Committee on Public Accounts (PAC) considered this matter on April 17, 2007 and agreed with our recommendation.

Agreement for information technology services needed

In chapter 7 of our 2006 Report – Volume 3, we reported that PSC needs an agreement with the Information Technology Office (ITO) for services it receives from ITO.

Since March 2006, PSC has used the ITO for certain information technology services without a signed agreement. At August 31, 2007, PSC had not yet signed such an agreement.

A written agreement is essential so that the PSC can effectively monitor services the ITO provides and take corrective or follow-up action as necessary such as adjustments to its processes or policies.

[1] PSC's human resource guidelines do not require departments to include assignments of responsibility and deadlines for implementing major strategies.

PAC considered this matter on April 17, 2007 and agreed with our recommendation.

We continue to recommend that the Public Service Commission sign a service-level agreement with the Information Technology Office for information technology services.

Leading human resources planning—a follow-up

This section explains that as of August 2007, PSC has addressed adequately two audit recommendations we made in 2005. Our 2005 Report – Volume 1, Chapter 2 described PSC's processes to lead human resource planning. In that report, we recommended that PSC:

- communicate to departments a manageable number of human resource priorities
- use a risk management framework to identify and analyze human resource risks and set acceptable risk levels

The Standing Committee on Public Accounts agreed with our recommendations on June 21, 2005.

Communicating priorities to departments

PSC communicated to departments a reasonable number of priorities for action in 2007. During its planning process, PSC seeks input from all departments. It identifies priorities in response to the requests of departments and input from the Cabinet. It also communicates often with departments about priorities.

Each year, PSC reviews trends and gives departments an *Environmental Scan* that highlights the importance of some issues. For 2007-08, PSC highlighted four themes described as having the greatest impact (i.e., leadership, talent management, employee engagement, and delivery of human resource services).

PSC emphasizes priorities in its *2006-10 Human Resource Plan* often using these themes. The goals and objectives in the *Plan* highlight the Government's human resource priorities. The *Plan* further assists departments to identify priorities by stating in which years PSC expects departments to take action on the identified issues.

Using a risk management framework

PSC now uses a risk management process that addresses the three elements that we recommended. PSC's process guides departments to identify risks, analyze risks (e.g., probability, consequences), and assess acceptable risk levels.

PSC's *Environmental Scan* and other guidelines encourage departments to identify internal or external risks. In its 2005 presentation, PSC named four major types of human resources risks that each department should consider (i.e., strategic, operational, financial, and compliance risks). PSC could further strengthen its guidance by using these four types of risks as a framework to help departments identify a wide range of human resources risks. Detailed examples within this framework would help departments systematically and efficiently recognize significant human resource risks.

PSC's 2007-08 *Human Resources Planning Guidelines* provide good guidance on analyzing risks and assessing risk levels.

Controls over MIDAS HR/payroll

Given PSC's overall responsibility for the MIDAS HR/Payroll module, it must have adequate central controls to secure MIDAS HR/Payroll and its information. Central controls are those controls that PSC must establish and carry out to protect the confidentiality, integrity, and availability of MIDAS HR/Payroll transactions.

Our audit objectives and criteria

We assessed the following:

♦ the adequacy of the conversion of data from the old computerized human resource and payroll systems (i.e., HRS (Human Resource System) and IPS (Internet Personnel System)) to the MIDAS HR/Payroll system

- whether PSC had adequate central controls to secure transactions on the MIDAS HR/Payroll system for the period from March 14, 2006 to December 31, 2006

To make these assessments, we used criteria based upon the *Trust Services Criteria and Principles* authored by The Canadian Institute of Chartered Accountants, international standards, literature, and reports of other legislative auditors. PSC agreed with the criteria.

Our criteria, set out in the Exhibit 1 below, describe the key processes that we expect PSC to have.

Exhibit 1

Adequate central controls to protect the confidentiality, integrity, and availability of transactions on MIDAS HR/Payroll must include control processes that:

1. **show management commitment to security (governance)**

   1.1 Responsibilities for security are clearly defined
   1.2 Management identifies threats and risks
   1.3 Management has approved security policies and procedures
   1.4 Management monitors security

2. **protect MIDAS HR/Payroll systems and data from unauthorized access**

   2.1 User access controls protect MIDAS HR/Payroll from unauthorized access
   2.2 Physical security controls protect MIDAS HR/Payroll from unauthorized access

3. **have MIDAS HR/Payroll systems and data available for operation**

   3.1 System and data backups occur and are tested
   3.2 Disaster recovery plans are in place and tested

4. **maintain the integrity of MIDAS HR/Payroll systems and data**

   4.1 Management has policies and procedures for managing MIDAS – HR/payroll
   4.2 Change management processes exist and are followed
   4.3 Processes for converting data exist and are followed
   4.4 Management monitors MIDAS HR/Payroll to ensure operating as planned

In this section, we call government agencies that use MIDAS HR/Payroll system “user agencies”. User agencies rely on PSC to have adequate central controls and to carry them out properly. User agencies also have responsibilities related to information processed within this system. For example, user agencies are responsible for the accuracy of data entered into the system and for assigning appropriate system access to their staff.

This audit did not assess the adequacy of controls at the user agencies. Rather, it focused on central processes at PSC to ensure MIDAS HR/Payroll was functioning properly.

Throughout our audit, we followed *The Standards for Assurance Engagements* established by The Canadian Institute of Chartered Accountants.

Our audit conclusions and findings

PSC adequately converted data from the old computerized human resource and payroll systems to MIDAS HR/Payroll.

PSC had adequate controls to protect the confidentiality, integrity, and availability of MIDAS HR/Payroll system for the period March 14, 2006 to December 31, 2006 except:

- **PSC did not have adequate policies and procedures for monitoring user access to the system, documenting and testing changes to the system, and providing user agencies with adequate reports to efficiently monitor and approve payroll**

- **PSC did not test its disaster recovery plan**

For each criteria, the following sets out what we expect (in italics), what we found, and related recommendation(s), if any.

Show management commitment to security

We expect PSC to show management commitment to security. Commitment includes setting up a strong organizational structure that clearly defines who is responsible for security. A strong IT division is led by a member of senior management. It is separate from the finance and operating divisions. It has a steering committee to ensure the IT division meets client needs. Commitment also includes implementing and monitoring compliance with security policies and procedures.

PSC has set up an effective IT organizational structure for securing MIDAS HR/Payroll. Staff roles and responsibilities are clearly defined.

Staff meet regularly to discuss MIDAS HR/Payroll issues. PSC has developed security policies and procedures for MIDAS HR/Payroll.

A steering committee, co-chaired by PSC and the Department of Finance, meets regularly to discuss operations and issues with MIDAS HR/Payroll.

PSC has also set up processes to manage its relationship with user agencies. PSC meets monthly with representatives from user agencies to discuss related processes and issues.

Protect MIDAS HR/Payroll systems and data from unauthorized access

We expect PSC to have adequate physical access and user access processes to protect the MIDAS HR/Payroll from unauthorized access.

Good physical controls means protecting IT infrastructure from harm. Physical access controls protect all computers, network devices, disk drives, backup devices, and wiring from unauthorized access. For example, PSC must have processes to prevent unauthorized persons from entering facilities.

User access management means protecting information in the IT system from unauthorized access. Access management is more critical with the increased use of the Internet, on-line approvals, automated processes, and multiple agencies accessing MIDAS HR/Payroll.

User access controls ensure only approved people can use MIDAS HR/Payroll. A common example of a user access control is a username and a password. The username identifies the user and the password grants access. User agencies decide who should have access to their systems and data and what access they can have. They advise PSC of their decisions. User agencies then rely on PSC to make sure only approved employees have access to the system.

The access controls must also establish access rights. Access rights determine what information a user can see or use. Access rights can also segregate duties of employees.

PSC has good physical security controls for protecting MIDAS HR/Payroll. PSC has contracted SaskTel to operate and protect access to the computer networks related to the MIDAS HR/Payroll system. Under its contract with SaskTel, PSC receives an audit report annually on the adequacy of SaskTel's related controls. Also, PSC secures its offices after hours.

PSC has clearly defined user roles within MIDAS HR/Payroll and appropriately separated the duties of each of these roles. User agencies are responsible for assigning roles to their staff in a way that is appropriate based on their operations and needs.

PSC has processes for granting and removing user access to MIDAS HR/Payroll. For example, only authorized persons at a user agency can approve requests to change user access including new hires and terminations. PSC determines whether the change request is properly authorized before it changes a user's access.

For the period of our audit, PSC did not have a process for periodically reviewing user access. For example, PSC should require each agency to confirm periodically that its users continue to have appropriate access. PSC did not do this and as a result, we found terminated employees that still had access to MIDAS HR/Payroll.

The confidentiality and integrity of MIDAS HR/Payroll depends on both PSC and each user agency protecting the system from unauthorized access. PSC must have processes to monitor user access assigned by user agencies to MIDAS HR/Payroll, and to take corrective action where access may no longer be appropriate.

2. We recommend the Public Service Commission have policies and procedures for monitoring user access to MIDAS HR/Payroll.

Management told us in, July 2007, PSC has implemented a process to have user agencies review and approve user access periodically.

Ensure MIDAS HR/Payroll systems and data are available for operation

We expect PSC to have strong processes to ensure MIDAS HR/Payroll systems and data are available for operation when needed. To reduce the amount of downtime for MIDAS HR/Payroll, PSC needs good backup and recovery procedures.

Even with good backup and recovery procedures, MIDAS HR/Payroll may not be able to continue its operations if a major problem occurs. Therefore, PSC should have strong contingency plans to recover operations in the event of a disaster like a fire or flood.

PSC has adequate backup procedures and does backups daily. To ensure its backups will be available in the event of a disaster, PSC keeps its backups offsite.

PSC has developed and approved a disaster recovery plan to restore MIDAS HR/Payroll in the event of a disaster. However, PSC has not tested the plan to ensure that MIDAS HR/Payroll will operate properly if a disaster occurs.

3. We recommend the Public Service Commission test its disaster recovery plan for MIDAS HR/Payroll.

Management told us in, July 2007, PSC had completed disaster recovery testing for MIDAS HR/Payroll.

Ensure the integrity of the MIDAS HR/Payroll systems and data

We expect PSC to have processes for maintaining the integrity of MIDAS HR/Payroll systems and data by implementing strong change management and operational processes. Processes would include the approval and testing of system changes before implementation and management of the MIDAS HR/Payroll system. Also, we expect PSC to monitor MIDAS HR/Payroll to ensure it operates as planned.

PSC had an adequate process for converting data from the old HRS and IPS payroll systems to MIDAS HR/Payroll.

PSC has developed policy and procedure manuals to help staff perform their MIDAS HR/Payroll related responsibilities. However, PSC needs to keep these manuals up-to-date as processes change. PSC has trained its staff and user-agency staff to use MIDAS HR/Payroll.

PSC has adequate processes for making changes to its systems. PSC has developed change management policy and procedures and uses a change management committee, which meets weekly to review changes. However, PSC did not always document its testing or approval of testing for changes to the system. Therefore, we do not know what tests were completed for changes, who approved the testing, or the test results.

4. We recommend that the Public Service Commission document and test changes to the MIDAS HR/Payroll system.

User agencies are responsible for the accuracy of the information they enter into MIDAS HR/Payroll. PSC retains responsibility for the accuracy of the processing of the information entered.

PSC has started to develop processes for managing MIDAS HR/Payroll to ensure it operates as planned. It carries out reconciliations to determine the accuracy of processing of information entered by user agencies.

MIDAS HR/Payroll has validation processes for data entered by user agencies such as timecard information. This limits the risk of user agencies entering unreasonable data. However, MIDAS HR/Payroll does not have built-in validation processes (edit checks) for all key data. Nor does MIDAS HR/Payroll automatically report or highlight to user agencies all instances where an employee’s payroll amount is in excess of a reasonable amount (reasonability checks). For example, during the year, a former employee received a vacation payout approximately $120,000 above the amount owed. The Government recovered the overpaid money. However, use of edit checks (such as dollar amount limits on vacation payouts) or reasonability checks may have prevented the error.

During the year, payroll reports were available to user agencies that outlined the net pay for all employees after each pay run. However, these reports did not help user agencies to identify errors or exceptions efficiently. Without such exception reports, user agencies cannot easily tell if data they have entered into the system is incorrect. This increases the risk that employees may be paid incorrect amounts without timely detection by the user agency.

The Financial Administration Act, 1993 requires proper approval of all payments for goods and services, including payroll, by an authorized person. Under the old human resource/payroll system, authorized signers reviewed and approved reports produced by HRS. MIDAS HR/Payroll does not produce similar reports to assist user agencies to approve payroll payments in accordance with section 30 of *The Financial Administration Act, 1993.*

5. **We recommend that the Public Service Commission provide user agencies with reports from MIDAS HR/Payroll to help them monitor the accuracy of payroll and approve payroll payments in accordance with *The Financial Administration Act, 1993.***

Management told us that reports are being developed to provide additional details needed to monitor payroll payments. Management also told us that during system development, they considered additional database edits but decided not to introduce such edits because they were not supported by the software vendor.

Selected references for controls over MIDAS/HR payroll

Canadian Institute of Chartered Accountants. (CICA). (2003). *Trust services principles and criteria*. Toronto: Author.

Canadian Institute of Chartered Accountants. (CICA). (1998). *Information technology control guidelines*. Toronto: Author.

International Organization for Standardization. (2005). ISO/IEC 17799:2005(E). *Information technology – Code of practice for information security management; 2nd Edition*. Geneva: Author.

The Information Systems Audit and Control Foundation. (2005). *CoBiT-governance, control and audit for information and related technology; 4th Edition*. Rolling Meadows, IL: Author.