Public Service Commission

9

Main points

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

PSC is responsible for the computerized human resources and payroll system. This system contains personnel and payroll information. PSC had adequate central controls to protect the confidentiality, integrity, and availability of transactions on this system with two exceptions. First, it did not have adequate policies and procedures for monitoring user access to the system. Second, PSC did not provide user agencies with updated written guidance over the approval of payroll payments and sufficient information to help them monitor the accuracy of their payroll.

Introduction

Under *The Public Service Act, 1998*, the Public Service Commission (PSC) provides leadership and policy direction for the human resource management of staff employed primarily by government ministries. Government ministries employ more than 12,000 staff working in permanent full-time, permanent part-time, term and labour service positions.[1]

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

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

This chapter contains the results of our audit of PSC's central controls to secure transactions on the Multi-informational Database Applications human resources and payroll system (MIDAS HR/Payroll). Our 2008 Report – Volume 3 will include the results of the rest of our audit work at PSC.

Controls over MIDAS HR/payroll

Background

Since March 2006, PSC is responsible for the MIDAS HR/Payroll system. At March 31, 2008, 22 ministries used MIDAS HR/Payroll to manage employee information (e.g., benefits, salary, job assignment, and training) and process payroll transactions for themselves and about 20 other government agencies.

Given PSC's overall responsibility for the MIDAS HR/Payroll system, it must have adequate central controls to secure MIDAS HR/Payroll and its information. Central controls are those controls that PSC must establish

[1] Saskatchewan Public Service Commission website (accessed April 3, 2008).

and carry out to protect the confidentiality, integrity, and availability of MIDAS HR/Payroll transactions.

Our audit objective and criteria

The objective of our audit was to assess whether PSC had adequate central controls to protect the confidentiality, integrity, and availability of transactions on MIDAS HR/Payroll for the twelve-month period ending December 31, 2007.

To make these assessments, we used criteria based on the *Trust Services Criteria and Principles* authored by The Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants, as well as international standards, literature, and reports of other legislative auditors. PSC has 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 – Audit criteria

Adequate central controls to protect the confidentiality, integrity, and availability of transactions 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 systems and data from unauthorized access**
   - 2.1. User access controls protect the system and data from unauthorized access
   - 2.2. Physical security controls protect the system and data from unauthorized access
3. **Make 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 systems and data**
   - 4.1. Management has policies and procedures for managing the system and data
   - 4.2. Change management processes exist and are followed
   - 4.3. Management monitors system to ensure it is operating as planned

In this chapter, we call the ministries that use MIDAS HR/Payroll "user agencies." User agencies rely on PSC, as a service provider, to have adequate central controls, carry them out properly, and have responsibilities related to processing data within the system accurately.

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 conclusion and findings

PSC had adequate central controls to protect the confidentiality, integrity, and availability of transactions on MIDAS HR/Payroll for the twelve-month period ended December 31, 2007 except:

- **PSC needs policies and procedures for monitoring user access to MIDAS HR/Payroll**
- **PSC needs to provide user agencies with updated written guidance over the approval of payroll payments in accordance with *The Financial Administration Act, 1993*, and MIDAS HR/payroll reports to help them monitor the accuracy of payroll and approve payroll payments in accordance with *The Financial Administration Act, 1993***

The following sets out our expectations (in italics) and significant findings.

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, physical control processes 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. Both service providers (i.e., PSC) and user agencies have responsibilities for protecting the system from unauthorized access. Service providers must have processes to monitor system user access assigned by user agencies and take corrective action where access may no longer be appropriate.

User access controls limit access to systems and data. A common example of a user access control is use of usernames and passwords. A username identifies the user and the password grants access. User access controls also establish access rights. Access rights determine what information a user can see or use. Access rights can also segregate duties of employees. User agencies decide which employees should have access to their systems and data and what access rights they can have. Service providers (e.g., PSC) must provide access only as directed and approved by user agencies.

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

PSC has clearly defined roles for users within MIDAS HR/Payroll and has appropriately separated the duties of users for 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.

Except for inactive accounts, PSC has sound processes for granting and removing user access to MIDAS HR/Payroll based on direction received from user agencies. For example, PSC accepts requests to change user access (including changes because of new hires and terminations) only from those persons at a user agency authorized to approve such requests. PSC determines whether the user agency's change request is properly authorized before making the change.

Since December 2007, PSC has required user agencies to carry out periodic reviews of their users' access to MIDAS HR/Payroll. It asks each user agency to confirm that access for users listed on a report it provides is appropriate. However, PSC does not ask user agencies to review their inactive user accounts and it does not automatically deactivate access of inactive users. We found a number of instances where user access was not removed in a timely manner.

Reviewing inactive user accounts is often referred to as a 'stale account process'. Such a process identifies user accounts not used within a certain timeframe (e.g., 90 days) and either automatically cancels or requires action from the user agency to continue access to these accounts. This reduces the risk of unauthorized access.

We previously reported this matter in our 2007 Report – Volume 3 (Chapter 20).

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

Maintain 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 include approving and testing system changes before implementation and managing the IT system to ensure it operates as planned.

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

Under *The Financial Administration Act, 1993* (Act), s.28 "every payment out of the general revenue fund is to be made…in the manner that the Provincial Comptroller may direct or approve." This includes payroll payments. The Act also expects that an authorized individual, before

making payment, certify that the services have been provided and that the amount to be paid and its payment is in accordance with the contract (e.g., terms of employment).[2]

The Financial Administration Manual (FAM) provides user agencies with general guidance on processing and approving payroll payments[3] and directs them to the more detailed guidance in PSC's policy and procedure manuals. PSC's policy and procedure manuals and guides (including guidance posted on the PSC MIDAS website) do not include explicit guidance on processing and approving payroll payments to ensure compliance with the Act. User agencies need written guidance to ensure payroll payments are processed and approved in accordance with the Act.

2. We recommend the Public Service Commission provide user agencies with written guidance on the processing and approval of payroll payments in accordance with *The Financial Administration Act, 1993*.

PSC has adequate processes for making changes to its systems. These processes include a written change management policy, procedures, and use of a change management committee that meets weekly to review changes. PSC tests and approves changes to the system.

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

During 2007, PSC 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 at user agencies.

Built-in validation processes and automatic reporting to user agencies of unusual data can limit the risk of an IT system processing unreasonable data. MIDAS HR/Payroll has built-in validation processes (edit checks) for some data entered by user agencies (such as timecard information) but not all key data. PSC told us that it does not plan to develop additional

[2] *The Financial Administration Act, 1993*, s.30 "Certification".
[3] For example, FAM sections 3120 and 3122.

edit checks. This lack of edit checks increases the need for reports to help determine the accuracy of data entered.

User agencies are responsible for the accuracy of the data entered into MIDAS HR/Payroll each pay period and approval of the payroll each pay period in accordance with the Act. MIDAS HR/Payroll does not automatically report or highlight to user agencies all instances where an employee's payroll amount is in excess of a reasonable amount (reasonability checks).

PSC recognized that user agencies need information each pay period to carry out their responsibilities. Each pay period, PSC made payroll reports available to user agencies prior to their staff being paid. These reports set out the net pay of each employee of the user agency for that pay period.

PSC expected user agencies to use these reports to confirm the accuracy of their payroll for each pay period (that is, to identify and follow up the entry of unusual data or potential data entry errors) prior to staff being paid. In 2007, PSC also expected user agencies to have processes to approve the payroll each pay period prior to staff being paid.

However, some user agencies found that the available reports did not contain sufficient information to enable them to detect errors or unusual pay amounts efficiently. Not providing user agencies with sufficient information increases the risk that user agencies may not detect incorrect or inappropriate data resulting in employees being paid at incorrect amounts.

We previously reported this matter in our 2007 Report – Volume 3 (Chapter 20).

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

During 2007, PSC consulted with user agencies to develop a revised report that would enable them to monitor payroll and identify errors and

exceptions more readily. PSC expanded the information in the report based on needs identified by the user agencies. The revised report contains sufficient information to enable user agencies to approve payroll payments in accordance with the Act. PSC made this report available to user agencies in February 2008. PSC has also developed another report for user agencies which highlights payroll payments in excess of reasonable amounts.

Selected references

Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA). (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 27002:2005(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.