Saskatchewan Association of Health Organizations

2E

This page left blank intentionally.

Introduction

The primary business of Saskatchewan Association of Health Organizations (SAHO) is to provide leadership, support, and services that will assist its membership in effectively delivering a comprehensive range of health services to the people of Saskatchewan[1]. Its members are the various healthcare providers within the Province. The largest members are the Regional Health Authorities (RHAs).

SAHO provides human resource and payroll services to almost all health care agencies in the province. SAHO processes payroll for approximately 37,000 people. Last year, the total payroll expenditures from the payroll system exceeded $1.2 billion. The RHAs incur the majority of the payroll expenditures. The RHAs must ensure they have adequate financial controls and reporting. SAHO provides payroll services on a cost recovery basis. SAHO has a Human Resource Management Steering Committee represented by members from the RHAs. The Steering Committee makes recommendations to management of SAHO about changes to the human resource and payroll system.

The payroll system is comprised of three separate computer systems known as Payroll Front End (PFE), Batch Calculations (BATCH), and Internet Personnel Front End (IPFE). PFE is a system some SAHO members use to transfer payroll data to SAHO for processing. This system is several years old and is in the process of being replaced. BATCH does all payroll calculations. BATCH also maintains data such as sick day and vacation accruals. IPFE is designed to replace PFE. In addition to allowing SAHO members to transfer information to BATCH, IPFE also stores all payroll transactions processed. Therefore, SAHO members can use IPFE for reporting purposes.

For the year ended March 31, 2006, SAHO had total expenses of $15 million (unaudited), an annual operating deficit of $0.4 million (unaudited), and held assets of $11.3 million (unaudited).

This chapter describes our audit of the SAHO payroll system for the period January 1, 2006 to March 31, 2006.

[1] *SAHO 2003-04 Annual Report*.

Our audit objective and criteria

The objective of our audit was to assess whether SAHO had adequate central controls to secure transactions on the payroll system for the period January 1, 2006 to March 31, 2006. The central controls are SAHO's policies and procedures for ensuring the security, integrity, and availability of the payroll system.

We use criteria to assess SAHO's processes. The criteria are based upon the *Trusted Services Criteria and Principles* authored by The Canadian Institute of Chartered Accountants, international standards, literature, and reports of other legislative auditors. SAHO agreed with the criteria.

Our criteria, set out in the Exhibit below, describe the key processes that we expected SAHO to use to secure transactions on its payroll system.

Exhibit 1—Audit criteria for securing the payroll system

To ensure SAHO has adequate central controls to secure transactions on the payroll system, SAHO should:

1. **Show management commitment to security (governance)**
   - 1.1 Responsibility for security is clearly defined
   - 1.2 A threat and risk assessment has been performed
   - 1.3 IT planning supports security
   - 1.4 Management has approved policies and procedures to secure the SAHO payroll system
   - 1.5 Management monitors security
   - 1.6 Service level agreements set out security, processing, and availability requirements
2. **Protect the payroll system from unauthorized access**
   - 2.1 User access is adequate to protect the payroll system from unauthorized access
   - 2.2 Physical security is adequate to protect the payroll system from unauthorized access
3. **Ensure the payroll system is available for operation**
   - 3.1 System and data backups occur and are tested
   - 3.2 Disaster recovery and business continuity plans are in place
4. **Ensure the integrity of payroll transaction processing**
   - 4.1 Change management processes exist and are followed
   - 4.2 Computer operation processes exist and are followed

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

Our conclusions

We found that SAHO had adequate controls to secure its payroll system for the period January 1, 2006 to March 31, 2006 except SAHO needs to monitor security controls for its service providers to protect SAHO's systems and data, strengthen security for its payroll system, and appropriately test and document payroll system changes.

We are not able to report on the adequacy of controls for IPFE because SAHO does not have adequate processes to identify, evaluate, and monitor its information technology (IT) service provider's security controls and we were not able to audit the service provider directly.

SAHO uses an IT service provider to develop, manage, and host the IPFE system. If IPFE is not available, SAHO and its members would not be able to process payroll transactions or review payroll reports. Also, if the service provider's security controls are not adequate, the confidentiality and integrity of data on IPFE could be at risk.

Key findings by criteria

Show management commitment to security (governance)

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 IT meets the agency's needs. Also an agency needs to monitor its security processes and those processes done by service providers to ensure that security is adequate to protect systems and data.

SAHO has setup an effective IT organizational structure. It is led by a member of senior management. SAHO also has a steering committee that is comprised of SAHO and client members. The committee meets

regularly to discuss IT issues related to the payroll system and identify system changes and enhancements.

SAHO needs to effectively monitor its service providers to ensure that security is adequate to protect systems and data as described below.

SAHO needs to monitor the IPFE service provider

SAHO needs to monitor the security controls provided by the service provider that maintains and hosts IPFE.

SAHO needs to implement processes to identify, evaluate, and monitor the service provider's user access, physical access, availability, change management, and computer operation controls.

Without strong monitoring processes, SAHO can not ensure that the IPFE system and payroll transaction data is secure, will be available when needed, or that the service provider is effectively providing services to SAHO.

1. We recommend the Saskatchewan Association of Health Organizations (SAHO) monitor the security controls of its Internet Personnel Front End service provider to protect SAHO's systems and data.

SAHO needs to monitor its external network service provider

SAHO needs to monitor the security controls provided by its external network service provider.

SAHO has an agreement with a service provider to provide security and data transmission services for SAHO. The service provider did not provide an expected security service for SAHO during the audit period. Also, the service provider does not provide any assurances on the security of SAHO data travelling on its network.

As a result of these weaknesses, SAHO does not know that its systems are protected from unauthorized users. Also, SAHO does not know its data transmitted on the service provider's network is secure or the network will be available when needed.

2. We recommend the Saskatchewan Association of Health Organizations (SAHO) monitor the security controls of its external network service provider to protect SAHO's systems and data.

Protect the payroll system from unauthorized access

We expect SAHO to ensure it has adequate physical access and user access processes to protect the payroll system 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, SAHO's buildings should be locked after hours and have processes to physically prevent unauthorized persons from entering facilities during working hours.

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, and automated processes.

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 gives access.

The access controls must also establish access rights. Access rights determine what systems, information, and applications a user can see or use. Access rights can also segregate duties within an application. When contractors obtain access to a SAHO system, they should follow SAHO's standards and be closely monitored. Finally, all access should be for a limited time and be reviewed periodically.

SAHO has good physical security controls for protecting its IT infrastructure. These controls are designed to ensure that unauthorized users do not obtain access to SAHO's facilities.

SAHO needs to improve its user access processes as described below.

Security policies and procedures needed

SAHO needs security policies and procedures for its information systems.

SAHO has made good progress in improving its security policies and procedures. SAHO's policies and procedures now identify who is responsible for the security of systems and data, define how access to systems is given or removed, and clearly identify the rules that staff need to follow. SAHO also did a security awareness training session for staff during the year.

SAHO has developed a plan for implementing its security policies and procedures. SAHO will need to ensure that it makes staff aware of and monitors compliance with its security policies and procedures.

We reported this matter in a previous report. In March 2006, the Standing Committee on Public Accounts agreed with our recommendation.

We continue to recommend that SAHO prepare, approve, and implement written security policies and procedures for its information systems.

SAHO needs to strengthen security for its payroll system

SAHO needs to ensure it has strong security processes to protect its systems and data. This includes ensuring that only authorized users have appropriate access to the systems and data. Also, SAHO needs to secure access to systems and data from non SAHO locations, follow established password standards, and protect its systems from known security risks.

Without strong security processes, SAHO can not ensure the confidentiality, integrity, and availability of the payroll system and data.

3. We recommend Saskatchewan Association of Health Organizations only allow authorized users access to its systems and data, follow established password standards, and protect its systems from known security risks.

Ensure the payroll system is available for operation

We expect SAHO to have strong processes to ensure the payroll system is available for operation when needed.

The availability of IT systems requires an agency to have good backup and recovery processes. This will ensure that systems and data can be restored in the event of a minor failure.

Even with good backup and recovery procedures, an agency may not be able to continue its operations if a major problem occurred. Therefore, agencies should have strong contingency plans to recover operations in the event of a disaster like a fire or flood. This includes building capacity, when cost effective, into systems so a disaster in one location will not cause applications to quit running at other locations where employees are still able to work.

SAHO has good backup and recovery processes. These processes ensure that backups are done daily and stored offsite. SAHO has implemented a backup payroll system in another city. The purpose of the backup system is to ensure that the payroll system can continue to provide services if the primary system fails. SAHO tested its backup site in December 2005. SAHO plans to test the backup site every six months to ensure it works as planned.

Regular testing of the backup system is needed to ensure it will work as planned. Also, as noted earlier, SAHO needs to monitor its service providers to ensure that a service provider's failure would not impact SAHO's ability to continue to deliver payroll services. Currently, a failure by the IPFE service provider or the external network service provider could make SAHO's payroll system unavailable even with a backup site.

Ensure the integrity of the payroll transaction processing

We expect SAHO to have strong processes for maintaining the integrity of the payroll system and related data. This includes processes for documenting, testing, approving, and moving changes from a test system to the payroll system. There should also be a quality assurance review after the change is complete. The quality assurance process ensures standards are met.

The payroll system started in 1973. SAHO took responsibility for the payroll system starting in 1995. To make sure the system continues to meet user needs, SAHO will need to make changes to its payroll systems on a regular basis. If a system change does not follow strong change management processes, the system may not work as planned or the accuracy and completeness of data may be at risk.

SAHO has developed policies and procedures for developing, testing, and implementing system changes. SAHO now needs to implement these policies and procedures.

SAHO needs to appropriately test and document payroll system changes

SAHO needs to ensure changes to its systems are appropriately tested to ensure the integrity and availability of its systems.

SAHO requires test plans to be documented and approved. SAHO told us that it shredded all test plans and test results due to space requirements. Therefore, we do not know what tests were completed for a change, who completed the testing, or the test results.

Without strong testing processes, SAHO can not ensure the integrity and availability of its systems.

4. We recommend that Saskatchewan Association of Health Organizations appropriately test and document payroll system changes.

Selected references

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

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.

The Information Systems Audit and Control Foundation. (2000). *CoBiT-Governance, Control and Audit for Information and Related Technology 3rd Edition*. Rolling Meadows, IL: Author.

This page left blank intentionally.