Justice and Attorney General

8

Main points

The Saskatchewan Legal Aid Commission (Commission) is a Crown agency of the Ministry of Justice and Attorney General. Each year, the Commission provides over 21,000 applicants in financial need with legal advice and representation. It uses information technology (IT) systems to help deliver these services. The Commission must protect the confidentiality, integrity, and availability of these systems and data stored within them.

We assessed the adequacy of the Commission's processes used to protect its systems and data. We found the Commission needs to:

- update its IT security policies and procedures based on a risk assessment
- physically secure its network computers located in area offices
- follow its password standards and monitor user access to its systems
- adequately configure, update, and monitor its computers and network equipment
- store, secure, and test its backup of information stored on its computers
- develop and test a disaster recovery plan for its information systems and data

Introduction

The mandate of the Department of Justice (effective November 21, 2007 the Department became the Ministry of Justice and Attorney General (Justice)) is to uphold the rule of law, protect basic legal rights of citizens, and ensure good and proper administration of justice[1]. Justice provides legal services for the Government and the people of Saskatchewan. Justice also administers registry systems for corporations and local registrars, and regulates pensions, credit unions, and businesses.

Justice is responsible for the operations of several trust and special purpose funds and Crown agencies including the Saskatchewan Legal Aid Commission.

This chapter contains the results of our audit of the adequacy of the Saskatchewan Legal Aid Commission's processes to secure its information technology (IT) environment.

Processes to secure its IT environment

The Saskatchewan Legal Aid Commission (Commission) was established on September 1, 1983 pursuant to *The Legal Aid Act*. The Commission provides legal advice and representation to people (clients) who meet the criteria defined in the Legal Aid Regulations, 1995. Generally, any person who receives social assistance is eligible to receive legal services.

The Commission provides legal services to over 21,000 applicants in financial need each year. The Commission plans to spend about $18 million in 2007-08.[2]

The Commission has one central office and 14 area offices. The central office includes the Commission's senior management team. The central office manages human resources and financial administration. The area offices provide legal services to clients. The Commission's computer system stores privileged client information in each area office. The Commission recognizes it must keep privileged information secure and maintain the availability and integrity of its legal systems and data.

[1] Saskatchewan Justice, 2006-2007 Annual Report, pg. 4.
[2] Annual Report 2006-07, Saskatchewan Legal Aid Commission, pp. 15-16.

The Commission uses a contractor to manage its network and deliver information technology (IT) services. For example, the contractor installs new equipment and updates computers against known security threats. While the contractor manages most IT controls, area offices perform some IT controls. For example, each area office has a staff member responsible for making secured copies (backups) of privileged client data.

To protect the Commission's systems and support their effective use, the Commission must have adequate controls for its network and data. Unauthorized disclosure, loss, or inappropriate modification of information could harm legal aid clients.

Audit objective and criteria

The objective of our audit was to assess whether the Saskatchewan Legal Aid Commission had adequate processes to secure its information technology environment for the period from November 1, 2007 to January 31, 2008. The Commission's information technology environment includes its computers, systems, data, and network equipment.

We used criteria to assess the Commission's processes. We based the criteria on the *Trust Services Criteria and Principles* authored by The Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants, international standards, literature, and reports of other legislative auditors. The Commission agreed with the criteria.

The criteria, set out in the exhibit below, describe the key processes that we expected the Commission to use to secure client systems and data.

Exhibit 1 — Audit criteria

To secure its information technology environment for the period from November 1, 2007 to January 31, 2008, the Commission should:

1. **Show management commitment to security**

   Responsibility for security is clearly defined
   Information Technology planning supports security
   Management has approved security policies and procedures
   Management monitors security

2. **Protect systems and data from unauthorized access**

   Physical security controls protect legal offices from unauthorized access
   User access controls protect the systems and data from 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

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

Audit conclusion

The Saskatchewan Legal Aid Commission had adequate processes to secure its information technology environment for the period November 1, 2007 to January 31, 2008 except for the matters described in the recommendations below.

Key findings by criterion

We describe below what we expect (in italics) and key findings for each criteria.

Show management commitment to security

Commitment includes setting up an organizational structure that clearly defines who is responsible for security. A member of senior management leads an information technology (IT) division. It has a steering committee *to ensure the IT division meets client needs. Management effectively monitors contractors who perform work on its behalf. Commitment also includes implementing and monitoring compliance with security policies and procedures.*

A senior staff member has responsibility for IT. The senior staff member oversees a contractor who performs IT work for the Commission. The Commission retains the responsibility for the security and availability of its systems and data. The contractor does not store or retain any Commission systems or data.

The Commission works closely with the contractor to set priorities and determine work plans. The contractor makes changes to systems and is responsible for keeping the systems and data available. The contractor does not regularly perform security assessments on the Commission's systems and data.

The Commission approved a three-year IT strategic plan in 2007. Senior management, key resources at the area offices, and contract resources worked together to prepare the plan. The Commission also has an IT steering committee that meets quarterly.

The Commission has some policies and procedures to protect its systems and data. However, the Commission's existing policies are outdated and not based on its risks. For example, the Commission does not have policies and procedures for updating, monitoring, or configuring its systems. The Commission needs to develop a complete set of policies and procedures for its systems and data based on a risk assessment. The Commission then needs to share the policies and procedures throughout the agency so that employees are aware of their security responsibilities.

1. We recommend the Saskatchewan Legal Aid Commission update its information technology security policies and procedures based on a risk assessment.

Protect systems and data from unauthorized access

We expect the Commission to have adequate physical access and user access processes that protect the systems and data 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, the Commission should physically prevent unauthorized users from entering its data centre.

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, automated processes, and multiple area offices. The Commission should protect its data by configuring, updating, and monitoring its systems against security threats.

The Commission has area offices throughout the province. All area offices have locks on the outside doors to prevent unauthorized access during non-working hours. However, the Commission does not have consistent security requirements at area offices. For example, we observed that some area offices leave outside security doors open. Open security doors allow unauthorized access to an area office.

Each area office uses a central network computer (server) to store legal data. Only two offices secure their server in a locked server room. For all other locations, the server and backup tapes (electronic copies of data stored) are readily available to anyone who gains physical access to the office. Also, the Commission does not have policies and procedures related to the transportation or safe storage of backup tapes.

2. We recommend that the Saskatchewan Legal Aid Commission physically secure network computers (servers) located in its area offices.

The Commission has an informal process for granting and removing user access to its IT systems and data. However, the Commission does not have documented policies and procedures for granting and removing user access. The Commission should document its processes to help protect against unauthorized user access.

The Commission's password policy is adequate. However, the Commission needs to consistently follow password standards, restrict the use of administrator accounts, and disable or remove inactive accounts. For example, approximately 15 staff share the administrator account and the password is not regularly changed.

The Commission does not monitor failed access attempts to its network, periodically review user accounts for appropriateness, or securely store master passwords. For example, only one person knows the master password for key network equipment. If that person was not available, the Commission would not have access to key network equipment. The Commission should store master user account information in a secure location so that it will be available if needed.

3. We recommend the Saskatchewan Legal Aid Commission follow its password standards and monitor user access for its systems.

The Commission has a computer network that could provide an appropriate foundation for secure service delivery. To provide for a secure network, the Commission needs to properly configure its computers and network equipment (e.g. firewalls). The Commission also needs to update its systems and network equipment against known security threats and provide effective monitoring.

The Commission needs to secure its network equipment. For example, the Commission's network equipment had configuration weaknesses that could allow an unauthorized user to gain access to its systems and data. The Commission also needs to strengthen its remote access processes.

The Commission has adequate processes to protect it from a computer virus. The Commission is also improving the security of its staff computers and network servers. For example, the Commission plans to encrypt all data stored on its laptop computers.

The Commission strengthened its processes for updating its servers during the audit period. However, the Commission does not have processes for updating its network equipment. The Commission needs to update its network equipment for known security risks.

The Commission does not log or monitor its network equipment that protect its systems and data. The Commission cannot identify attempted or successful security breaches on a timely basis without an adequate review of log information.

4. We recommend the Saskatchewan Legal Aid Commission adequately configure, update, and monitor its computers and network equipment.

Keep systems and data available for operation

We expect the Commission to have adequate processes to ensure its systems and data are available for operation when needed.

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 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.

The Commission stores privileged legal information at each area office. Each area office is responsible for performing daily backups of this information. The contractor provides assistance upon request by an area office.

The Commission needs to implement effective processes for storing, securing, and testing backups. We found that some area offices do not store data backups offsite. This could result in an area office's data being lost in the event of a disaster. The area offices that do store backups offsite need improved security controls. For example, data backups should not be stored in unsecure areas. The Commission also needs to perform tests to check whether the data backups worked successfully.

Without adequately securing and testing its backups, the Commission is at risk of loss or disclosure of privileged client information.

The Commission does not have an up-to-date disaster recovery plan. The Commission needs to prepare a plan based on a threat and risk assessment.

The Commission has been able to restore individual systems and data when required (for example, when files are lost or computers replaced). However, without an approved and tested plan, the Commission does not know if it could restore all systems and data in the event of a disaster. This could result in systems, data, and services being unavailable when needed.

5. **We recommend the Saskatchewan Legal Aid Commission adequately store, secure, and test its backups of information stored on its computers.**

6. **We recommend the Saskatchewan Legal Aid Commission develop and test a disaster recovery plan for its information systems and data.**

Maintain the integrity of systems and data

We expect the Commission to have processes for maintaining the integrity of client systems and data by implementing adequate change management and IT operation processes. Adequate processes require approving and testing system changes before implementation. The Commission also needs to ensure that it has adequate processes for running and maintaining its computers.

The Commission lacks adequate processes for configuring, updating, and monitoring its systems and data. We describe these findings and recommendations earlier under the heading “Protect systems and data from unauthorized access.”

Selected references

Canadian Institute of Chartered Accountants (CICA) & American Institute of Certified Public Accountants (AICPA). (2007). For Security, Availability, Processing Integrity, Confidentiality, and Privacy. (Including WebTrust® and SysTrust™). In *Trust services principles and criteria*. Toronto: Author. http://www.cica.ca/index.cfm/ci_id/38256/la_id/1. (25 Apr 2008)

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

Information Systems Audit and Control Foundation. (2005). *CoBiT4.0*. Rolling Meadows, IL: Author.

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). *Information technology – Code of practice for information security management; 1st Edition*. Geneva: Author.

IT Governance Institute. (2006). IT Control Objectives for Sarbanes-Oxley: *The role of IT in the design and implementation of internal control over financial reporting, 2nd Edition*. Rolling Meadows, IL: Author.

This page left blank intentionally.